ELSEVIER

Theoretical Computer Science 269 (2001) 231–282

Theoretical Computer Science

www.elsevier.com/locate/tcs

An axiomatic semantics for Esterel ☆

Simone Tini

Dipartimento di Informatica, Università di Pisa, Corso Italia 40, 56125, Pisa, Italy

Received February 2000; revised October 2000; accepted November 2000
Communicated by M. Nivat

Abstract

In this paper we propose an axiomatic semantics for the synchronous language Esterel. We begin with giving a structural operational semantics for Esterel in terms of a labeled transition system (LTS). We prove that bisimulation on LTS states (which correspond to Esterel programs) is a congruence and that our LTS reflects the input/output behavior of programs. So, bisimilar programs are distinguished neither by any Esterel context nor by the external environment, and bisimulation is a reasonable notion of behavioral equivalence. In order to characterize equivalent programs, we give a set of axioms and we prove that they induce an axiomatization over Esterel which is sound and complete modulo bisimulation. © 2001 Elsevier Science B.V. All rights reserved.

Keywords: Esterel; Synchronous languages; Equivalences; Axiomatic semantics

1. Introduction

Esterel [12, 11] is an imperative *synchronous language* [5, 19] tailored for programming *reactive systems* [21], namely systems which maintain an ongoing interaction with their environment at a rate controlled by this. Esterel is based on the *synchronous hypothesis* [12], which states that a reactive system is able to react instantaneously and in no time to stimuli from the external environment, so that outputs from the system are available as soon as inputs from the environment are. The synchronous hypothesis is indeed an abstraction and amounts to requiring that the system is faster than its environment.

The operational and denotational semantics of Esterel have been developed in [12, 11, 17], respectively. Moreover, in [11] the so-called *circuit semantics* of Esterel has been proposed. Esterel programs are mapped to sequential circuits, compositionally

☆ Research partially supported by MURST progetto cofinanziato "TOSCA".
E-mail address: tini@di.unipi.it (S. Tini).

PII: S0304-3975(00)00420-5

w.r.to program structure. Circuits may be interpreted both as a semantic model of Esterel and as an implementation of the language.

We aim to give an axiomatic semantics of Esterel, in order to characterize behaviorally equivalent programs. As it is well known, axiomatic semantics may be used for transformation of programs and for proof by rewriting.

Firstly, we need a notion of behavioral equivalence over Esterel programs. It is reasonable to require that equivalent programs are distinguished neither by the external environment nor by any Esterel context.

For this purpose, we give a *structural operational semantics* [28] for Esterel in terms of a *labeled transition system* (LTS) [22, 28] with LTS states corresponding to programs and LTS transitions corresponding to program reactions, and then we consider the *bisimulation* [27, 25] on the LTS as a behavioral equivalence over Esterel programs. We prove that the bisimulation on our LTS is a congruence and that our LTS reflects the input/output behavior of programs. So, bisimilar programs are distinguished neither by any Esterel context nor by the external environment. To prove that our LTS reflects the input/output behavior of programs, we prove that from the LTS we can recover the input/output behavior of circuits corresponding to programs, namely, we prove that our LTS interpretation agrees with the circuit semantics of [11].

To axiomatize Esterel, we provide a system of axioms defining an equality relation over Esterel programs. We prove that this equality relation is sound and complete modulo bisimulation, in the sense that two arbitrary programs are equated if and only if they are bisimilar.

To prove the completeness of our axiomatization, we introduce a notion of normal form of programs, we prove that every program can be transformed into a bisimilar normal form by applying our axioms, and we prove that bisimilar normal forms are equated by our axioms. The idea of exploiting normal forms to prove completeness of axiomatizations is well established in the field of asynchronous process algebras (as examples, see [8, 24]). In the asynchronous setting, normal forms are nondeterministic sequential processes called *head normal forms*. Concurrency is reduced to sequentiality plus nondeterminism, because actions of processes running in parallel can arbitrarily interleave. We cannot adopt this approach because, in the synchronous setting, programs running in parallel proceed at the same rate and their actions do not interleave. As a consequence, concurrency cannot be simulated by nondeterminism and no notion of head normal form can be considered. As normal forms, we consider programs of the form $P_1 \| \ldots \| P_n$, where "$\|$" is the commutative and associative operator of parallel composition, and $P_1, \ldots, P_n$ are sequential programs. The syntactic structure of our normal forms is such that, given a normal form $P_1 \| \ldots \| P_n$ and an input from the environment, $P_1, \ldots, P_n$ react, but at most one of them will be able to react to the next input.

The paper is organized as follows. In Section 2, we recall Esterel and some well-known notions on the semantics of programming languages. In Section 3, we define our LTS and we prove that bisimulation is a congruence. In Section 4, we give our axioms and we prove their soundness and completeness modulo bisimulation. In Section 5, we

prove that the LTS reflects the circuit semantics of [11]. Finally, in Section 6 we draw some conclusions.

2. Background

In this section we recall some classic notions on the semantics of programming languages, and we give an overview of the language Esterel. We refer to [3, 11] for more complete treatments.

2.1. Structural operational semantics

We begin with reviewing the model of labeled transition systems [22, 28] and the notion of bisimulation [25, 27].

Definition 1. A *labeled transition system* (LTS) is a tuple $\langle S, L, \{\xrightarrow{l} \mid l \in L\}\rangle$, where S is a set of *states*, L is a set of *labels*, and $\xrightarrow{l} \subseteq S \times S$ is a *transition relation* for every $l \in L$.

Following standard notation, we write $s_1 \xrightarrow{l} s_2$ for $(s_1, s_2) \in \xrightarrow{l}$, and we say that $s_1 \xrightarrow{l} s_2$ is a *transition*. We write $s_1 \xrightarrow{l}$ if there is a transition $s_1 \xrightarrow{l} s_2$ for some state s_2, and $s_1 \not\xrightarrow{l}$ if there is no transition $s_1 \xrightarrow{l} s_2$ for any state s_2. We will identify an LTS with the collection of its transitions.

Definition 2. Given an LTS $\langle S, L, \{\xrightarrow{l} \mid l \in L\}\rangle$, a relation $R \subseteq S \times S$ is a *bisimulation* if whenever $s_1 R s_2$:
(1) if $s_1 \xrightarrow{l} s_1'$ then there exists a transition $s_2 \xrightarrow{l} s_2'$ such that $s_1' R s_2'$;
(2) if $s_2 \xrightarrow{l} s_2'$ then there exists a transition $s_1 \xrightarrow{l} s_1'$ such that $s_1' R s_2'$.

A bisimulation is an equivalence relation. The union of all bisimulations on the states of an LTS is a bisimulation and is denoted by $\approx$.

Sometimes, an equivalent definition of bisimulation is given. Given a relation $R \subseteq S \times S$, let us denote by $\mathscr{F}(R)$ the relation on S containing all pairs (s_1, s_2) satisfying conditions 1 and 2 of Definition 2. Now, R is a bisimulation iff $R \subseteq \mathscr{F}(R)$.

We recall now the notion of terms over a signature.

Let us consider a countable set of *variables* $\mathtt{Var}$, ranged over by x, y, z. A *signature* Σ is a set of *function symbols*, disjoint from $\mathtt{Var}$, together with an *arity* mapping that assigns a natural number $ar(f)$ to each function symbol f.

Definition 3. The set of (*open*) *terms* $\mathtt{T}(\Sigma)$ over a signature Σ is the least set such that:
- each variable $x \in \mathtt{Var}$ is a term;
- if f is a function symbol and $t_1, \ldots, t_{ar(f)}$ are terms, then $f(t_1, \ldots, t_{ar(f)})$ is a term.

The set $\mathtt{T}(\Sigma)$ is ranged over by t, u. Terms that do not contain variables are called *closed terms*. The abstract syntax of process description languages is usually given by a signature Σ. Closed terms are called *processes*.

A *substitution* is a mapping $\sigma : \mathtt{Var} \to \mathtt{T}(\Sigma)$. A substitution extends to a mapping from terms to terms, namely, $\sigma(t)$ is the term obtained by replacing occurrences of variables x in term t by $\sigma(x)$.

We introduce now the notions of transition system specification and of transition provable from a transition system specification [18].

Definition 4. Let us assume a signature Σ and a set of labels L. A *transition rule* (*with positive premises*) ρ is of the form H/α, where H is a collection of *premises* of the form $t \xrightarrow{l} t'$, α is a *conclusion* of the form $t \xrightarrow{l} t'$, with t, t' ranging over $\mathtt{T}(\Sigma)$, and l over L.

A *transition system specification* (TSS) is a collection of transition rules.

Given a conclusion $t \xrightarrow{l} t'$ of a transition rule ρ, t and t' are called the *source* and the *target* of ρ, respectively. If both t and t' are closed terms, then $t \xrightarrow{l} t'$ is called a *closed transitions*.

Definition 5. Let T be a TSS. A *proof* from T of a closed transition $t \xrightarrow{l} t'$ is a well-founded, upwardly branching tree whose nodes are labeled by closed transitions, whose root is labeled by $t \xrightarrow{l} t'$, and, if K is the (possibly empty) set of labels of the nodes directly above a node labeled by β, then K/β is a closed substitution instance of a transition rule in T.

A closed transition $t \xrightarrow{l} t'$ is *provable* from T iff there is a proof of $t \xrightarrow{l} t'$ from T.

The meaning of a TSS with positive premises T is the LTS having as transitions the set of the closed transitions provable from T.

We recall now the notion of positive GSOS format [13] for transition rules.

Definition 6. A transition rule ρ is in *positive GSOS format* if

$$\rho = \frac{\{x_i \xrightarrow{l_{ij}} y_{ij} \mid 1 \leqslant i \leqslant ar(f), 1 \leqslant j \leqslant m_i\}}{f(x_1, \ldots, x_{ar(f)}) \xrightarrow{l} t},$$

where $m_i \geqslant 0$, and the variables x_i and y_{ij} are all distinct and the only variables occurring in ρ.

A TSS is in *positive GSOS format* if it consists of positive GSOS rules only.

We recall that, given a signature Σ, an equivalence relation R over closed terms is a *congruence* iff, for every function symbol $f \in \Sigma$, we have

$$t_i \, R \, u_i \text{ with } 1 \leqslant i \leqslant ar(f) \text{ implies } f(t_1, \ldots, t_{ar(f)}) R f(u_1, \ldots, u_{ar(f)}).$$

The following result stems from [13].

Theorem 7. *Bisimulation on an LTS induced by a positive GSOS TSS is a congruence.*

We recall now the notion of sum of TSSs [18].

Definition 8. Let T_0 and T_1 be TSSs whose signatures Σ_0 and Σ_1 agree on the arity of the function symbols in $\Sigma_0 \cap \Sigma_1$. The *sum* of T_0 and T_1, denoted $T_0 \oplus T_1$, is the TSS over $\Sigma_0 \cup \Sigma_1$ containing the transition rules in $T_0 \cup T_1$.

A question that naturally arises is whether or not the LTSs induced by T_0 and $T_0 \oplus T_1$ contain the same transitions $t \xrightarrow{l} t'$, for t closed term over Σ_0.

The following definition stems from [33].

Definition 9. A TSS $T_0 \oplus T_1$ is an *operational conservative extension* of T_0 if, for any closed term t over Σ_0, if a transition $t \xrightarrow{l} t'$ is provable from $T_0 \oplus T_1$, then $t \xrightarrow{l} t'$ is provable also from T_0.

The following definition stems from [15].

Definition 10. The *source-dependent* variables in a transition rule ρ are defined inductively as follows:

- all variables in the source of ρ are source-dependent;
- if $t \xrightarrow{l} t'$ is a premise of ρ and all variables in t are source-dependent, then all variables in t' are source-dependent.

A transition rule is *source-dependent* if all its variables are.

The following theorem, which is a consequence of a result given in [15], formulates sufficient criteria for a TSS $T_0 \oplus T_1$ to be an operational conservative extension of T_0.

Theorem 11. *Let T_0 and T_1 be TSSs over signatures Σ_0 and Σ_1 such that $T_0 \oplus T_1$ is defined. Under the following conditions, $T_0 \oplus T_1$ is an operational conservative extension of T_0:*

- *each transition rule in T_0 is source-dependent;*
- *the source of each transition rule in T_1 contains a function symbol in $\Sigma_1 \setminus \Sigma_0$.*

We recall that a *conditional axiomatization* over a signature Σ consists of a set of conditional equations, called (*conditional*) *axioms*, of the form

$$t_0 = u_0 \Leftarrow t_1 = u_1, \ldots, t_n = u_n$$

with $t_i, u_i \in \mathrm{T}(\Sigma)$, $0 \leqslant i \leqslant n$, and $n \geqslant 0$.

An axiomatization gives rise to a binary equality relation $=$ on $\mathrm{T}(\Sigma)$ s.t.:

- if $t_0 = u_0 \Leftarrow t_1 = u_1, \ldots, t_n = u_n$ is an axiom and σ is a substitution such that $\sigma(t_i) = \sigma(u_i)$, $1 \leqslant i \leqslant n$, then $\sigma(t_0) = \sigma(u_0)$;

- the relation $=$ is closed under reflexivity, symmetry and transitivity;
- if $f \in \Sigma$ is a function symbol and $t_i = u_i$, $1 \leqslant i \leqslant ar(f)$, then

$$f(t_1, \ldots, t_{ar(f)}) = f(u_1, \ldots, u_{ar(f)}).$$

Note that relation $=$ is an equivalence and a congruence.

Definition 12. Given a signature Σ, let us assume a relation of equivalence $\sim$ over closed terms and an axiomatization $\mathscr{A}$ over Σ.

- $\mathscr{A}$ is *sound* modulo $\sim$ if $t = u$ implies $t \sim u$, for t, u closed terms.
- $\mathscr{A}$ is *complete* modulo $\sim$ if $t \sim u$ implies $t = u$, for t, u closed terms.

2.2. An overview of Esterel

Esterel is a synchronous language suitable for programming hardware or software controllers for which the control handling aspects are predominant. An Esterel program (*module*) has a body, consisting of an imperative *statement*, and an interface w.r.to the environment, consisting of a set of input signals, denoted with I, and of a set of output signals, denoted with O. Signals local to the body may be used for internal communications. Signals are *pure*, namely they carry only their presence/absence status.

As in [9, 11], we interpret Esterel as the process algebra having the terms (statements) generated by the following BNF-like grammar:

$$\begin{aligned} E ::= {} & \texttt{nothing} \mid \texttt{emit}\ s \mid \texttt{pause} \mid \texttt{present}\ s\ \texttt{then}\ E\ \texttt{else}\ E\ \texttt{end} \mid E \parallel E \mid \\ & E\,;E \mid \texttt{signal}\ s\ \texttt{in}\ E\ \texttt{end} \mid \texttt{loop}\ E\ \texttt{end} \mid \texttt{suspend}\ E\ \texttt{when}\ s \mid \\ & \texttt{trap}\ T\ \texttt{in}\ E\ \texttt{end} \mid \texttt{exit}\ T, \end{aligned}$$

where s ranges over a finite set of signal names $\mathscr{S} = \{s_1, \ldots, s_{|\mathscr{S}|}\}$, and T ranges over a finite set of trap names $\mathscr{T} = \{T_1, \ldots, T_{|\mathscr{T}|}\}$. We say that `nothing`, `pause`, `emit` and `exit` are *basic* statements. We will denote by $\equiv$ the syntactic identity over statements.

A module behaves cyclically in an input-driven way: at each cycle it reads the status of input signals and reacts by executing the current statement, so that both the status of output signals and the statement to be executed at the subsequent cycle are determined. According to the *synchronous hypothesis*, reactions take no time and outputs become available as soon as inputs are (i.e. in the same cycle). Since reactions are instantaneous, Esterel constructs take no time, except the delay statement `pause` which takes precisely one unit of time. So, when a statement *starts*, either it executes a statement `exit` T in its body and *exits* the *trap* T, so that the body of `trap` T terminates immediately, or it executes a statement `pause` in its body and it *pauses*, or it *terminates* immediately. A pausing statement will be *resumed* at the subsequent cycle.

Informally, `nothing` does nothing and terminates immediately. This means that `nothing` terminates in the cycle in which it starts.

Statement `emit` s sets status of the output signal s to "present" and terminates immediately. At every execution cycle, local signals and output signals are present if and only if some corresponding statement `emit` is executed.

Statement `pause` pauses for one cycle. It will be resumed at the subsequent one and it will terminate immediately.

Statement `present` s `then` E_1 `else` E_2 `end` behaves either as E_1, if the input signal s is present, or as E_2, otherwise.

Statement $E_1; E_2$ is the sequencing of E_1 and E_2. As ";" takes no time, if E_1 terminates then E_2 starts immediately.

Statement $E_1 \| E_2$ is the synchronous parallel composition of E_1 and E_2. Due to the synchronous hypothesis, E_1 and E_2 are perfectly synchronized and their actions cannot arbitrarily interleave. (For this reason it is said that the synchronous hypothesis reconciles concurrency and determinism [12].) As an example, let $E_1 \equiv$ `emit` s_1; `pause`; `emit` s_1' and $E_2 \equiv$ `emit` s_2; `pause`; `emit`; s_2'. At the first cycle, both s_1 and s_2 are emitted, and at the second cycle both s_1' and s_2' are emitted. We cannot have interleaving: s_1' cannot be emitted before s_2.

Statement `signal` s `in` E `end` declares s to be local to E. The output signal s of E is fed back to the input signal s of E. This feedback is instantaneous, namely if E emits s then s is immediately sensed by E. As an example, let $E \equiv$ `emit` $s \|$ `present` s `then emit` s' `else nothing end`. The left branch of E emits s, which is immediately (i.e. in the same cycle) sensed by the right branch, which can emit s'.

Statement `loop` E `end` executes infinitely E. It is required that the body of a `loop _ end` cannot terminate immediately (i.e. in the cycle in which it starts). This restriction ensures that the computation in every cycle is finite (see [12, 11]).

Statement `suspend` E `when` s behaves as E at the first execution cycle. At subsequent cycles, if s is present then the execution of E is suspended for one cycle, else E receives the control.

Finally, `trap` T `in` E `end` defines the scope of trap T, and `exit` T causes the immediate termination of its body. As an example, let $E \equiv$ `present` s `then exit` T `else nothing end`; E'. If s is present then the whole statement terminates and E' is not performed.

2.2.1. Constructiveness

It is well known that instantaneous feedback may originate *paradoxes of causality* between signals, so that *reactivity* and *determinism* may be lost.

Reactivity is the ability of a statement to react to any input from the environment. As an example, the statement

```
signal s in (present s then nothing else emit s end) end
```

is nonreactive (namely, it cannot perform any reaction), because the local signal s is emitted if and only if it is absent at the same instant, so that it cannot assume any status.

Determinism is the ability of a statement to have a unique reaction to any input from the environment. As an example, the statement

```
signal s in (present s then emit s else nothing end) end
```

is nondeterministic, because s is emitted if and only if it is present at the same instant, so that it could coherently assume either status present or absent.

The static semantics of Esterel [12] rejects nonreactive and nondeterministic statements, since reactivity and determinism are needed in programming synchronous controllers [10]. In [11] the notion of *constructiveness* has been introduced. Constructiveness is the ability to determine the status of local and output signals, without making any assumption on them, by a fact-to-fact propagation, starting from the status of input signals. As an example, let us consider the statement

`signal` s `in (present` s `then emit` s `else emit` s `end) end`,

where the local signal s is emitted either if it is present or if it is absent at the same instant. This statement is reactive and deterministic, since s assumes status present, but it is nonconstructive. In fact, in order to deduce that s is present we must be sure that some `emit` s is executed. To infer that the `emit` s in the `then` branch of "`present` s" is executed, we must assume that s is present. So, to say that s is present, we assume this fact and then we check that this assumption is correct. This is counterintuitive, since it seems that what happens in a branch of a "`present` s" determines the choice of such branch, namely, some information flows backward w.r.to the sequential control. This is the reason why nonconstructive statements are rejected in [11].

3. The labeled transition system

In this section we propose an LTS as an operational semantic model for Esterel. LTS states correspond to Esterel statements, LTS transitions correspond to statement reactions, and LTS labels carry information on the status of input/output signals, on signal causality, and on the termination of statements.

In Section 3.1, we give the transition system specification defining the LTS and we prove that bisimulation is a congruence. In Section 3.2, we explain the meaning of the transition rules in detail. Finally, in Section 3.3, we compare our LTS with the LTSs for Esterel proposed in the literature.

3.1. The transition system specification

We begin with introducing some notations.

Let $\mathscr{S}_{-}^{+}$ be the set $\{s^{+}, s^{-} \mid s \in \mathscr{S}\}$. Given a signal $s \in \mathscr{S}$, the symbol s^{+} denotes the presence of s, while s^{-} denotes the absence of s. In the following, γ will range over $\mathscr{S}_{-}^{+}$. We assume a function $^{-} : \mathscr{S}_{-}^{+} \to \mathscr{S}_{-}^{+}$ such that $\overline{s^{+}} = s^{-}$ and $\overline{s^{-}} = s^{+}$, for every $s \in \mathscr{S}$.

An *event* S (over $\mathscr{S}$) is a subset of $\mathscr{S}_{-}^{+}$. It is *consistent* if for no signal s, both $s^{+} \in S$ and $s^{-} \in S$. Consistent events are assumptions over the status of signals. We write $S \uparrow S'$ if the union of events S and S' is a consistent event.

An *ordered event* ϑ (over $\mathscr{S}$) is a string in $(\mathscr{S}^+_-)^*$. We let ϑ, ϕ, ψ range over ordered events. Following the usual convention, we denote with ε the empty string. Given an ordered event ϑ, we denote with $|\vartheta|$ the event such that

$$|\vartheta| = \begin{cases} \emptyset & \text{if } \vartheta = \varepsilon, \\ \{\gamma\} \cup |\phi| & \text{if } \vartheta = \gamma\phi. \end{cases}$$

Definition 13. Given an ordered event ϑ and a symbol $\mu \in \{n, p\} \cup \mathscr{S} \cup \mathscr{T}$, $\vartheta\mu$ is a *causality term* with ϑ as *cause* and μ as *action*.

A causality term $\vartheta\mu$ refers to an atomic action performed by some statement if input signals have status as assumed by ϑ. Atomic actions may be: termination, denoted with n, pausing, denoted with p, production of a signal s, denoted with s, exiting a trap T, denoted with T. Action s subsumes the action of termination, in the sense that if a statement produces s then it terminates. A causality term ϑs highlights causality between signals.

Definition 14. A *label* is a tuple $l = \langle S_l, \mathscr{E}_l, \mathscr{N}_l, \mathscr{T}_l \rangle$ such that:
- S_l is a consistent event over $\mathscr{S}$;
- $\mathscr{E}_l$ is a set of causality terms such that, for each $\vartheta\mu \in \mathscr{E}_l$, $|\vartheta| \subseteq S_l$;
- $\mathscr{N}_l$ is a set of causality terms such that, for each $\vartheta\mu \in \mathscr{N}_l$, $|\vartheta| \not\subset S_l$;
- $\mathscr{T}_l \in \{0, 1\} \cup 2^{\mathscr{T}}$;
- if $\vartheta\mu \in \mathscr{E}_l \cup \mathscr{N}_l$, $\vartheta = \gamma_1 \cdots \gamma_m$, $\mu = n$, then $\gamma_m = s^+$ for some $s \in \mathscr{S}$.

We will denote with $\mathscr{L}$ the set of labels as in Definition 14.

An LTS transition $E \xrightarrow{l} F$ will represent the reaction of E to an environment that supplies every input signal s such that $s^+ \in S_l$ and does not supply any input signal s such that $s^- \in S_l$.

Causality terms in $\mathscr{E}_l$ refer to atomic actions that are performed during the reaction represented by $E \xrightarrow{l} F$. In particular, during this reaction E emits the set of signals $\{s \in \mathscr{S} | \vartheta s \in \mathscr{E}_l\}$, which will be denoted with $Em(l)$.

A causality term $\vartheta\mu$ is in $\mathscr{N}_l$ if it refers to an atomic action that is not performed, since either some input signal s with $s^+ \in |\vartheta|$ is absent or some input signal s with $s^- \in |\vartheta|$ is present. We will see that we need information in $\mathscr{E}_l$ and $\mathscr{N}_l$ to have the correspondence between our SOS semantics and the circuit semantics of [11] (see Lemmata 48 and 49).

The component $\mathscr{T}_l$ carries information about the termination of E, namely $\mathscr{T}_l = 0$ if E terminates, $\mathscr{T}_l = 1$ if E pauses, $\mathscr{T}_l \in 2^{\mathscr{T}}$ if E exits the outermost trap in $\mathscr{T}_l$.

The LTS is defined by the transition system specification in Table 1.

Rule *nothing* states that `nothing` terminates immediately. We will denote by δ the label $\langle \emptyset, \{\varepsilon n\}, \emptyset, 0 \rangle$. Rule *emit* states that `emit` s emits the signal s and terminates immediately. The causality term εs in label $\langle \emptyset, \{\varepsilon s\}, \emptyset, 0 \rangle$ emphasizes that s is emitted independently of the status of input signals. Rule *pause* states that `pause` pauses for

Table 1
The labeled transition system for Esterel

$$\frac{}{\texttt{nothing} \xrightarrow{\langle \emptyset, \{\varepsilon n\}, \emptyset, 0\rangle} \texttt{nothing}} \quad (nothing)$$

$$\frac{}{\texttt{emit}\ s \xrightarrow{\langle \emptyset, \{\varepsilon s\}, \emptyset, 0\rangle} \texttt{nothing}} \quad (emit)$$

$$\frac{}{\texttt{pause} \xrightarrow{\langle \emptyset, \{\varepsilon p\}, \emptyset, 1\rangle} \texttt{nothing}} \quad (pause)$$

$$\frac{}{\texttt{exit}\ T \xrightarrow{\langle \emptyset, \{\varepsilon T\}, \emptyset, \{T\}\rangle} \texttt{nothing}} \quad (exit)$$

$$\frac{E \xrightarrow{l} F}{\texttt{trap}\ T\ \texttt{in}\ E\ \texttt{end} \xrightarrow{tr(T,l)} \texttt{nothing}}\ \mathscr{T}_l = 0 \vee \mathscr{T}_l = \{T\} \quad (trap\_1)$$

$$\frac{E \xrightarrow{l} F}{\texttt{trap}\ T\ \texttt{in}\ E\ \texttt{end} \xrightarrow{tr(T,l)} \texttt{trap}\ T\ \texttt{in}\ F\ \texttt{end}}\ \mathscr{T}_l = 1 \quad (trap\_2)$$

$$\frac{E \xrightarrow{l} F}{\texttt{trap}\ T\ \texttt{in}\ E\ \texttt{end} \xrightarrow{tr(T,l)} \texttt{nothing}}\ \mathscr{T}_l \subseteq \mathscr{T},\ \mathscr{T}_l \neq \{T\} \quad (trap\_3)$$

$$\frac{E \xrightarrow{l} F \quad E' \xrightarrow{l'} F'}{\texttt{present}\ s\ \texttt{then}\ E\ \texttt{else}\ E'\ \texttt{end} \xrightarrow{s^+(l,l')} F}\ s^- \notin S_l \quad (present\_1)$$

$$\frac{E \xrightarrow{l} F \quad E' \xrightarrow{l'} F'}{\texttt{present}\ s\ \texttt{then}\ E\ \texttt{else}\ E'\ \texttt{end} \xrightarrow{s^-(l',l)} F'}\ s^+ \notin S_{l'} \quad (present\_2)$$

$$\frac{E \xrightarrow{l} F \quad E' \xrightarrow{l'} F'}{E \parallel E' \xrightarrow{l \otimes l'} F \parallel F'}\ S_l \uparrow S_{l'},\ \mathscr{T}_l, \mathscr{T}_{l'} \in \{0,1\} \quad (parallel\_1)$$

$$\frac{E \xrightarrow{l} F \quad E' \xrightarrow{l'} F'}{E \parallel E' \xrightarrow{l \otimes l'} \texttt{nothing}}\ S_l \uparrow S_{l'},\ \mathscr{T}_l \subseteq \mathscr{T} \vee \mathscr{T}_{l'} \subseteq \mathscr{T} \quad (parallel\_2)$$

$$\frac{E \xrightarrow{l} F \quad E' \xrightarrow{l'} F'}{E; E' \xrightarrow{l \triangleright l'} F'}\ \mathscr{T}_l = 0,\ S_l \uparrow S_{l'} \quad (seq\_1)$$

$$\frac{E \xrightarrow{l} F \quad E' \xrightarrow{l'} F'}{E; E' \xrightarrow{l \triangleright l'} F;\ E'}\ \mathscr{T}_l = 1 \quad (seq\_2)$$

$$\frac{E \xrightarrow{l} F \quad E' \xrightarrow{l'} F'}{E; E' \xrightarrow{l \triangleright l'} \texttt{nothing}}\ \mathscr{T}_l \subseteq \mathscr{T} \quad (seq\_3)$$

$$\frac{E \xrightarrow{l} F}{\texttt{signal}\ s\ \texttt{in}\ E\ \texttt{end} \xrightarrow{loc(s,l)} \texttt{signal}\ s\ \texttt{in}\ F\ \texttt{end}}\ loc(s,l) \in \mathscr{L} \quad (signal)$$

$$\frac{E \xrightarrow{l} F}{\texttt{loop}\ E\ \texttt{end} \xrightarrow{l} F; \texttt{loop}\ E\ \texttt{end}}\ \mathscr{T}_l = 1 \quad (loop\_1)$$

$$\frac{E \xrightarrow{l} F}{\texttt{loop}\ E\ \texttt{end} \xrightarrow{l} \texttt{nothing}}\ \mathscr{T}_l \subseteq \mathscr{T} \quad (loop\_2)$$

$$\frac{E \xrightarrow{l} F}{\texttt{suspend}\ E\ \texttt{when}\ s \xrightarrow{l} \texttt{nothing}}\ \mathscr{T}_l \neq 1 \quad (suspend\_1)$$

$$\frac{E \xrightarrow{l} F}{\texttt{suspend}\ E\ \texttt{when}\ s \xrightarrow{l} \texttt{suspend imm}\ F\ \texttt{when}\ s}\ \mathscr{T}_l = 1 \quad (suspend\_2)$$

one cycle and will behave as `nothing` at the subsequent one. Rule *exit* states that `exit` T exits the trap T.

Rule *trap_1* states that if E either terminates or exits the trap T, then `trap` T `in` E `end` terminates. Rule *trap_2* states that if E pauses, then so does `trap` T `in` E `end`. Rule *trap_3* states that if E exits a trap T' with `trap` T `in` E `end` in its body, then so does `trap` T `in` E `end`.

Rule *present_1* (resp. *present_2*) states that if s is present (resp. absent) then `present` s `then` E `else` E' `end` behaves as E (resp. E').

Rules *parallel_1* and *parallel_2* state that $E \| E'$ performs both a reaction of E and a reaction of E'. The derivative of $E \| E'$ is `nothing` if $E \| E'$ exits a trap, which happens if either E or E' does (rule *parallel_2*).

Rule *seq_1* states that if E terminates then E; E' performs both reactions of E and E'. Rules *seq_2* and *seq_3* state that if E either pauses or exits a trap then E; E' reacts as E. If E exits a trap then the derivative of E; E' is `nothing`.

Rule *signal* states that `signal` s `in` E `end` behaves as E, provided that s is a local signal.

Rules *loop_1* and *loop_2* state that `loop` E `end` behaves as E; `loop` E `end`. We do not consider the case with $\mathscr{T}_l = 0$ since the body of a `loop` cannot terminate.

As in [11], let us denote with `suspend imm` E `when` s the statement

`trap` T `in`

`loop present` s `then pause else exit` T `end end`

`end; suspend` E `when` s

which differs from `suspend` E `when` s since E can be suspended also at the first execution cycle. Rule *suspend_1* states that if E either terminates immediately or exits a trap, then so does `suspend` E `when` s. Rule *suspend_2* states that if E pauses, then so does `suspend` E `when` s. In this case, at the next execution cycle, if E behaves as F then `suspend` E `when` s will behave as `suspend imm` F `when` s.

The LTS describes the input/output behavior of statements: a transition $E \xrightarrow{l} F$ reflects that E reacts to input S_l by producing signals $Em(l)$. In order to relate Esterel statements having the same input/output behavior, we consider bisimulation relation on the states of the LTS.

The following theorem states that no Esterel context is able to distinguish between bisimilar statements, namely that Esterel constructs preserve bisimulation.

Theorem 15. *The bisimulation on Esterel statements is a congruence.*

Proof. Directly by Theorem 7 and the fact that the TSS in Table 1 is a positive GSOS TSS (cf. Definition 6). □

3.2. The meaning of the transition rules

Before explaining rules *present_1* and *present_2* we need some notations.

Given a set of causality terms Θ and an ordered event ϕ, we denote with Θ^{ϕ} the set of causality terms $\{\phi\vartheta\mu \mid \vartheta\mu \in \Theta\}$.

Given $l, l' \in \mathscr{L}$ and $\gamma \in \mathscr{S}_-^+$ such that $\bar{\gamma} \notin S_l$, we denote by $\gamma(l, l')$ the label:

$$\gamma(l,l') = \begin{cases} \langle S_l \cup \{\gamma\}, \mathscr{E}_l^{\gamma}, \mathscr{N}_l^{\gamma} \cup \mathscr{E}_{l'}^{\bar{\gamma}} \cup \mathscr{N}_{l'}^{\bar{\gamma}}, \mathscr{T}_l \rangle & \text{if } l \neq \delta \neq l', \\ \langle S_l \cup \{\gamma\}, \mathscr{E}_l^{\gamma}, \mathscr{N}_l^{\gamma}, \mathscr{T}_l \rangle & \text{if } l \neq \delta = l', \\ \langle S_l \cup \{\gamma\}, \emptyset, \mathscr{E}_{l'}^{\bar{\gamma}} \cup \mathscr{N}_{l'}^{\bar{\gamma}}, \mathscr{T}_l \rangle & \text{if } l = \delta \neq l', \\ \langle \{s^+\}, \{s^+ n\}, \emptyset, 0 \rangle & \text{if } l = \delta = l' \text{ and } \gamma = s^+, \\ \langle \{s^-\}, \emptyset, \{s^+ n\}, 0 \rangle & \text{if } l = \delta = l' \text{ and } \gamma = s^-. \end{cases}$$

Let us consider rule *present_1* (rule *present_2* is analogous). We have that $S_{s^+(l,l')} = S_l \cup \{s^+\}$ since the reaction represented by the transition labeled by $s^+(l, l')$ is caused by the presence of s and by the input causing the reaction of E.

Let us assume that $l \neq \delta \neq l'$. If $\vartheta\mu$ refers to an atomic action performed by a statement in the body of E, then $s^+\vartheta\mu$ appears in $s^+(l, l')$ and reflects that this atomic action requires the presence of s. If $\vartheta\mu$ refers to an atomic action performed by a statement in the body of E', then $s^-\vartheta\mu$ appears in $s^+(l, l')$ and reflects that this atomic action requires the absence of s. If $l \neq \delta = l'$ then we forget the causality term $s^- n$, since causality terms of the form $s^+\vartheta\mu$ implicitly keep track that if s is absent then a `nothing` is executed. The case with $l = \delta \neq l'$ is analogous. In both labels $s^+(\delta, \delta)$ and $s^-(\delta, \delta)$, the causality term $s^+ n$ appears. Another possible choice is to allow causality terms of the form $\vartheta s^- n$ and to have $s^-(\delta, \delta) = \langle \{s^-\}, \{s^- n\}, \emptyset, 0 \rangle$. Our choice permits to have $\mathscr{E}_l \cup \mathscr{N}_l = \mathscr{E}_{l'} \cup \mathscr{N}_{l'}$, for l and l' labels of two arbitrary transitions having the same LTS state as source state.

We have $\mathscr{T}_{s^+(l,l')} = \mathscr{T}_l$ since the whole statement terminates, pauses or exits a trap if E does it.

Note that the label $s^+(l, l')$ keeps track of signal causality arising from both branches of `present` s. We will see that this is needed to have correspondence between our SOS semantics and the circuit semantics of [11] (see Lemmata 48 and 49).

Example 16. Let us assume $E \equiv$ `present` s `then emit` s_1 `else emit` s_2 `end`.

By rule *present_1* we have $E \xrightarrow{l_1}$ `nothing`, with $l_1 = \langle \{s^+\}, \{s^+ s_1\}, \{s^- s_2\}, 0 \rangle$.

By rule *present_2* we have $E \xrightarrow{l_2}$ `nothing`, with $l_2 = \langle \{s^-\}, \{s^- s_2\}, \{s^+ s_1\}, 0 \rangle$.

As it will be stated by Proposition 26, $\mathscr{E}_{l_1} \cup \mathscr{N}_{l_1} = \mathscr{E}_{l_2} \cup \mathscr{N}_{l_2}$ for l_1 and l_2 labels of two arbitrary transitions having the same state as source. So, rule *present_1* does not depend on the choice of l', and rule *present_2* does not depend on the choice of l.

In rules *parallel_1* and *parallel_2* we assume a partial function $\otimes : \mathscr{L} \times \mathscr{L} \rightharpoonup \mathscr{L}$ such that, given labels l and l' such that $S_l \uparrow S_{l'}$, we have:

(1) $S_{l \otimes l'} = (S_l \cup S_{l'}) \setminus \{\gamma \mid \{\gamma, \bar{\gamma}\} \cap |\vartheta| = \emptyset$ for each $\vartheta\mu \in \mathscr{E}_{l \otimes l'} \cup \mathscr{N}_{l \otimes l'}\}$;

(2) $\mathscr{E}_{l \otimes l'} = (\mathscr{E}_l \cup \mathscr{E}_{l'}) \setminus (\{\vartheta\phi\, p, \vartheta\phi n \mid \vartheta\, p \in \mathscr{E}_l \cup \mathscr{E}_{l'} \cup \mathscr{N}_l \cup \mathscr{N}_{l'}\} \cup \{\vartheta\gamma n \mid$ either $\vartheta\gamma\phi\mu \in \mathscr{E}_l \cup \mathscr{E}_{l'} \cup \mathscr{N}_l \cup \mathscr{N}_{l'}$ or $\vartheta\bar{\gamma}\ \phi\mu \in \mathscr{E}_l \cup \mathscr{E}_{l'} \cup \mathscr{N}_l \cup \mathscr{N}_{l'}\})$;

(3) $\mathcal{N}_{l\otimes l'} = (\mathcal{N}_l \cup \mathcal{N}_{l'})\backslash(\{\vartheta\phi p, \vartheta\phi n \mid \vartheta p \in \mathcal{E}_l \cup \mathcal{E}_{l'} \cup \mathcal{N}_l \cup \mathcal{N}_{l'}\} \cup \{\vartheta\gamma n \mid$ either $\vartheta\gamma\phi\mu \in \mathcal{E}_l \cup \mathcal{E}_{l'} \cup \mathcal{N}_l \cup \mathcal{N}_{l'}$ or $\vartheta\bar{\gamma}\phi\ \mu \in \mathcal{E}_l \cup \mathcal{E}_{l'} \cup \mathcal{N}_l \cup \mathcal{N}_{l'}\})$;

(4)

$$\mathcal{T}_{l\otimes l'} = \begin{cases} \max(\mathcal{T}_l, \mathcal{T}_{l'}) & \text{if } \mathcal{T}_l, \mathcal{T}_{l'} \in \{0,1\}, \\ (\mathcal{T}_l \cup \mathcal{T}_{l'}) \cap \mathcal{T} & \text{otherwise.} \end{cases}$$

Function $\otimes$ is such that $l \otimes l'$ carries information given by both l and l'. We could define $\otimes$ by imposing $S_{l\otimes l'} = S_l \cup S_{l'}$, $\mathcal{E}_{l\otimes l'} = \mathcal{E}_l \cup \mathcal{E}_{l'}$ and $\mathcal{N}_{l\otimes l'} = \mathcal{N}_l \cup \mathcal{N}_{l'}$. Our choice permits to remove redundant information from labels and, as a consequence, to have a coarser notion of bisimulation on statements.

Since $E \,\|\, E'$ terminates if both E and E' do, if $\mathcal{T}_l = \mathcal{T}_{l'} = 0$ then $\mathcal{T}_{l\otimes l'} = 0$. Since $E \,\|\, E'$ pauses if either E pauses and E' does not exit any trap, or conversely, if $\mathcal{T}_l, \mathcal{T}_{l'} \in \{0,1\}$ and either $\mathcal{T}_l = 1$ or $\mathcal{T}_{l'} = 1$ then $\mathcal{T}_{l\otimes l'} = 1$. Since $E \,\|\, E'$ exits the outermost trap among those exited by E and E', if either $\mathcal{T}_l \subseteq \mathcal{T}$ or $\mathcal{T}_{l'} \subseteq \mathcal{T}$ then $\mathcal{T}_{l\otimes l'} \subseteq \mathcal{T}$. In the last case, the derivative of $E \,\|\, E'$ is `nothing`. Note that this derivative will never be executed, since $E \,\|\, E'$ is in the body of a `trap` that terminates immediately.

If both $\vartheta\phi p$ (resp. $\vartheta\phi n$) and ϑp are in $\mathcal{E}_l \cup \mathcal{E}_{l'} \cup \mathcal{N}_l \cup \mathcal{N}_{l'}$, then we forget $\vartheta\phi p$ (resp. $\vartheta\phi n$) which carries redundant information. In fact, when each signal s such that $s^+ \in |\vartheta|$ is present and each signal s such that $s^- \in |\vartheta|$ is absent, an action of pausing is performed by a statement in the body of $E \,\|\, E'$. So, the action of pausing (resp. termination) indicated by $\vartheta\phi p$ (resp. $\vartheta\phi n$) is useless.

Example 17. Let us assume $E \equiv \texttt{pause} \,\|\, (E_1 \,\|\, E_2)$, where
$E_1 \equiv \texttt{present}\ s_1\ \texttt{then pause else nothing end}$,
$E_2 \equiv \texttt{present}\ s_1\ \texttt{then nothing else nothing end}$.

We have $E \xrightarrow{l} \texttt{nothing}$, where $l = \langle \emptyset, \{\varepsilon p\}, \emptyset, 1\rangle$. Note that $E \approx \texttt{pause}$.

Note that we forget a causality term $\vartheta\phi p$ or $\vartheta\phi n$ such that $\vartheta\mu \in \mathcal{E}_l \cup \mathcal{E}_{l'} \cup \mathcal{N}_l \cup \mathcal{N}_{l'}$ only if $\mu = p$. To see the reason, let us consider the statement E' obtained by replacing all occurrences of `pause` in the statement E of Example 17 by `nothing`. In this case, either the presence or the absence of s_1 is needed to have the termination of E'. So, if we consider a statement $E'; E''$, with E'' arbitrary, either the presence or the absence of s_1 is needed to start E''. If, as an example, $E'' \equiv \textit{emit}\ z$, then we must keep track of the causality between s_1 and z.

If both $\vartheta\gamma n$ and $\vartheta\gamma\phi\mu$ (resp. $\vartheta\bar{\gamma}\phi\mu$) are in $\mathcal{E}_l \cup \mathcal{E}_{l'} \cup \mathcal{N}_l \cup \mathcal{N}_{l'}$ then we forget $\vartheta\gamma n$, since $\vartheta\gamma\phi\mu$ (resp. $\vartheta\bar{\gamma}\phi\mu$) keeps track of the fact that if each signal s such that $s^+ \in |\vartheta\gamma|$ is present and each signal s such that $s^- \in |\vartheta\gamma|$ is absent then an action is performed by some statement, so that the action of termination indicated by $\vartheta\gamma n$ is useless.

Example 18. Let us assume $E \equiv E_1 \,\|\, E_2$, where
$E_1 \equiv \texttt{present}\ s_1\ \texttt{then emit}\ s_2\ \textit{else}\ \texttt{nothing}$,
$E_2 \equiv \texttt{present}\ s_1\ \texttt{then nothing else nothing}$.

We have $E \xrightarrow{l_1}$ nothing and $E \xrightarrow{l_2}$ nothing, where $l_1 = \langle \{s_1^+\}, \{s_1^+ s_2\}, \emptyset, 0\rangle$ and $l_2 = \langle \{s_1^-\}, \emptyset, \{s_1^+ s_2\}, 0\rangle$. Note that $E \approx E_1$.

The following proposition implies that $E \,\|\, F \approx F \,\|\, E$, for E and F arbitrary Esterel statements. (This property will be used when proving the soundness of our axiomatization.)

Proposition 19. *Given labels l_1 and l_2, it holds $l_1 \otimes l_2 = l_2 \otimes l_1$.*

Proof. Directly by the definition of $\otimes$. □

The following proposition implies that $E \,\|\, (F \,\|\, G) \approx (E \,\|\, F) \,\|\, G$, for E, F and G arbitrary Esterel statements.

Proposition 20. *Given labels l_1, l_2 and l_3, it holds $l_1 \otimes (l_2 \otimes l_3) = (l_1 \otimes l_2) \otimes l_3$.*

Proof. We prove that $\mathscr{E}_{l_1 \otimes (l_2 \otimes l_3)} = \mathscr{E}_{(l_1 \otimes l_2) \otimes l_3}$. The proof that $\mathscr{N}_{l_1 \otimes (l_2 \otimes l_3)} = \mathscr{N}_{(l_1 \otimes l_2) \otimes l_3}$ is analogous, while the proofs that $S_{l_1 \otimes (l_2 \otimes l_3)} = S_{(l_1 \otimes l_2) \otimes l_3}$ and $\mathscr{T}_{l_1 \otimes (l_2 \otimes l_3)} = \mathscr{T}_{(l_1 \otimes l_2) \otimes l_3}$ are immediate.

We begin with proving that $\mathscr{E}_{l_1 \otimes (l_2 \otimes l_3)} \subseteq \mathscr{E}_{(l_1 \otimes l_2) \otimes l_3}$ by showing that causality terms in $\mathscr{E}_{l_i} \setminus \mathscr{E}_{(l_1 \otimes l_2) \otimes l_3}$ are in $\mathscr{E}_{l_i} \setminus \mathscr{E}_{l_1 \otimes (l_2 \otimes l_3)}$, for an arbitrary $1 \leqslant i \leqslant 3$.

If $\gamma_1 \ldots \gamma_i p \in \mathscr{E}_{l_i} \setminus \mathscr{E}_{(l_1 \otimes l_2) \otimes l_3}$ then $\gamma_1 \ldots \gamma_j p \in \mathscr{E}_{l_1} \cup \mathscr{E}_{l_2} \cup \mathscr{E}_{l_3}$ for some $j < i$.

If $\gamma_1 \ldots \gamma_j p \in \mathscr{E}_{l_1} \cup \mathscr{E}_{l_2 \otimes l_3}$ then $\gamma_1 \ldots \gamma_i p \notin \mathscr{E}_{l_1 \otimes (l_2 \otimes l_3)}$. In fact, either $\gamma_1 \ldots \gamma_i p$, $\gamma_1 \ldots \gamma_j p \in \mathscr{E}_{l_2} \cup \mathscr{E}_{l_3}$ and $\gamma_1 \ldots \gamma_i p$ is removed when computing $l_2 \otimes l_3$, or $\gamma_1 \ldots \gamma_i p$ is removed when computing $l_1 \otimes (l_2 \otimes l_3)$. Otherwise, there exists $\gamma_1 \ldots \gamma_h p \in \mathscr{E}_{l_1} \cup \mathscr{E}_{l_2 \otimes l_3}$ for some $h < j$, and, also in this case, $\gamma_1 \ldots \gamma_i p \notin \mathscr{E}_{l_1 \otimes (l_2 \otimes l_3)}$.

If $\gamma_1 \ldots \gamma_i n \in \mathscr{E}_{l_i} \setminus \mathscr{E}_{(l_1 \otimes l_2) \otimes l_3}$ then we have one of the following cases:

- $\gamma_1 \ldots \gamma_j p \in \mathscr{E}_{l_1} \cup \mathscr{E}_{l_2} \cup \mathscr{E}_{l_3}$ for some $j < i$. We reason as above.
- either $\gamma_1 \ldots \gamma_i \phi\mu \in \mathscr{E}_{l_1} \cup \mathscr{E}_{l_2} \cup \mathscr{E}_{l_3} \cup \mathscr{N}_{l_1} \cup \mathscr{N}_{l_2} \cup \mathscr{N}_{l_3}$ or $\gamma_1 \ldots \overline{\gamma_i} \phi\mu \in \mathscr{E}_{l_1} \cup \mathscr{E}_{l_2} \cup \mathscr{E}_{l_3} \cup \mathscr{N}_{l_1} \cup \mathscr{N}_{l_2} \cup \mathscr{N}_{l_3}$. Let us assume the first case. The other is analogous. If $\gamma_1 \ldots \gamma_i \phi\mu \in \mathscr{E}_{l_1} \cup \mathscr{E}_{l_2 \otimes l_3} \cup \mathscr{N}_{l_1} \cup \mathscr{N}_{l_2 \otimes l_3}$ then $\gamma_1 \ldots \gamma_i n \notin \mathscr{E}_{l_1 \otimes (l_2 \otimes l_3)}$. Otherwise, if $\mu \in \{n, p\}$ and $\psi p \in \mathscr{E}_{l_1} \cup \mathscr{E}_{l_2 \otimes l_3} \cup \mathscr{N}_{l_1} \cup \mathscr{N}_{l_2 \otimes l_3}$, for ψ a prefix of $\gamma_1 \ldots \gamma_i \phi\mu$, then, also in this case, $\gamma_1 \ldots \gamma_i n \notin \mathscr{E}_{l_1 \otimes (l_2 \otimes l_3)}$. Finally, if $\mu = n$, $\phi = \gamma'_1 \ldots \gamma'_m$, and either $\gamma_1 \ldots \gamma_i \gamma'_1 \ldots \gamma'_m \phi'\mu'$ or $\gamma_1 \ldots \gamma_i \gamma'_1 \ldots \overline{\gamma'_m} \phi'\mu'$ is in $\mathscr{E}_{l_1} \cup \mathscr{E}_{l_2 \otimes l_3} \cup \mathscr{N}_{l_1} \cup \mathscr{N}_{l_2 \otimes l_3}$, then, also in this case, $\gamma_1 \ldots \gamma_i n \notin \mathscr{E}_{l_1 \otimes (l_2 \otimes l_3)}$.

The proof that $\mathscr{E}_{l_1 \otimes (l_2 \otimes l_3)} \supseteq \mathscr{E}_{(l_1 \otimes l_2) \otimes l_3}$ is analogous. □

Before explaining rules *seq_1*, *seq_2*, *seq_3*, we need some notations.

Given an ordered event $\vartheta = \gamma_1 \ldots \gamma_m$, we denote with $\overline{\vartheta}$ the set of ordered events $\{\gamma_1 \ldots \gamma_{i-1} \overline{\gamma_i} \mid 1 \leqslant i \leqslant m\}$.

Given a statement E and a label l such that $\mathscr{E}_l \cup \mathscr{N}_l = \{\vartheta_1 \mu_1, \ldots, \vartheta_n \mu_n\}$ and $E \xrightarrow{l}$, we denote with $\mathscr{I}(E)$ the set of all ordered events ϕ of the form $\phi_{i_1} \ldots \phi_{i_n}$ such that,

for every

$$1 \leqslant j \leqslant n,\ \phi_{i_j} \in \begin{cases} \{\vartheta_{i_j}\} \cup \overline{\vartheta_{i_j}} & \text{if } \mu_{i_j} \notin \{p\} \cup \mathscr{T}, \\ \overline{\vartheta_{i_j}} & \text{otherwise.} \end{cases}$$

Note that, by Proposition 26, it follows that if $E \xrightarrow{l_1}$ and $E \xrightarrow{l_2}$, then $\mathscr{I}(E)$ can be computed indifferently by considering l_1 or l_2. For each ordered event $\phi \in \mathscr{I}(E)$, if the environment supplies each signal s such that $s^+ \in |\phi|$ and does not supply any signal s such that $s^- \in |\phi|$, then E terminates immediately. In fact, no statement `pause` or `exit` is executed. So, for a causality term $\vartheta'\mu'$ which refers to an atomic action performed by a statement in the body of E', $\phi\vartheta'$ gives one of the possible statuses of signals causing this atomic action.

Given a label l such that $E \xrightarrow{l}$, we denote with $\mathscr{I}(l)$ the set of ordered events $\{\phi \mid \phi \in \mathscr{I}(E) \text{ and } |\phi| = S_l\}$.

Example 21. Let us assume $E \equiv E_1 \parallel E_2$, where:
$E_1 \equiv$ `present` s_1 `then exit` T `else nothing end`,
$E_2 \equiv$ `present` s_2 `then emit` s_3 `else nothing end`.

We have $E \xrightarrow{l_i}$, $1 \leqslant i \leqslant 4$, where

$$l_1 = \langle \{s_1^+, s_2^+\}, \{s_1^+ T, s_2^+ s_3\}, \emptyset, \{T\} \rangle,$$
$$l_2 = \langle \{s_1^+, s_2^-\}, \{s_1^+ T\}, \{s_2^+ s_3\}, \{T\} \rangle,$$
$$l_3 = \langle \{s_1^-, s_2^+\}, \{s_2^+ s_3\}, \{s_1^+ T\}, 0 \rangle,$$
$$l_4 = \langle \{s_1^-, s_2^-\}, \emptyset, \{s_1^+ T, s_2^+ s_3\}, 0 \rangle.$$

We have $I(l_1) = \emptyset$, $I(l_2) = \emptyset$, $I(l_3) = \{s_1^- s_2^+, s_2^+ s_1^-\}$, $I(l_4) = \{s_1^- s_2^-, s_2^- s_1^-\}$, $I(E) = I(l_1) \cup I(l_2) \cup I(l_3) \cup I(l_4)$.

In rules *seq_1*, *seq_2* and *seq_3* we assume a partial function $\rhd : \mathscr{L} \times \mathscr{L} \rightharpoonup \mathscr{L}$ such that, given labels l and $l' \neq \delta$ such that $\mathscr{T}_l = 0$ implies $S_l \uparrow S_{l'}$, we have

$$l \rhd l' = \begin{cases} l \otimes \langle \emptyset, \emptyset, \bigcup_{\phi \in \mathscr{I}(E)} \mathscr{E}_{l'}^{\phi} \cup \mathscr{N}_{l'}^{\phi}, 0 \rangle & \text{if } \mathscr{T}_l \neq 0, \\ l \otimes \langle S_{l'} \bigcup_{\phi \in \mathscr{I}(l)} \mathscr{E}_{l'}^{\phi}, \bigcup_{\phi \in \mathscr{I}(E) \setminus \mathscr{I}(l)} \mathscr{E}_{l'}^{\phi} \cup \bigcup_{\phi \in \mathscr{I}(E)} \mathscr{N}_{l'}^{\phi}, \mathscr{T}_{l'} \rangle & \text{if } \mathscr{T}_l = 0. \end{cases}$$

Moreover, if $l' = \delta$, we assume $l \rhd l' = l$.

If $\mathscr{T}_l \neq 0$ then $S_{l \rhd l'} = S_l$, since the reaction of $E; E'$ is caused by the input causing the reaction of E. If $\mathscr{T}_l = 0$ then $S_{l \rhd l'} = S_l \cup S_{l'}$, since the reaction of $E; E'$ is caused by inputs causing the reactions of E and E'.

If $E \xrightarrow{l} F$, $\mathscr{T}_l \neq 0$, and $\phi \in \mathscr{I}(E)$, then $|\phi|$ is not consistent with S_l, as $|\phi| = S_{l''}$ for some l'' with $\mathscr{T}_{l''} = 0$. So, for each $\vartheta\mu \in \mathscr{E}_{l'} \cup \mathscr{N}_{l'}$, $\phi\vartheta\mu$ appears in $\mathscr{N}_{l \rhd l'}$.

If $E \xrightarrow{l} F$, $\mathscr{T}_l = 0$, and $\phi \in \mathscr{I}(E)$, then $|\phi|$ is consistent with S_l if and only if $|\phi| = S_l$. So, for $\vartheta\mu \in \mathscr{E}_{l'}$, $\phi\vartheta\mu \in \mathscr{E}_{l \rhd l'}$ if $|\phi| = S_l$ and $\phi\vartheta\mu \in \mathscr{N}_{l \rhd l'}$ otherwise. Moreover, if $\vartheta\mu \in \mathscr{N}_{l'}$, then $\phi\vartheta\mu \in \mathscr{N}_{l \rhd l'}$.

Since $E;E'$ pauses if E does, and since $E;E'$ exits a trap T if E does, if $\mathscr{T}_l \neq 0$ then $\mathscr{T}_{l \triangleright l'} = \mathscr{T}_l$. Since $E;E'$ has the same termination mode of E' when E terminates, if $\mathscr{T}_l = 0$ then $\mathscr{T}_{l \triangleright l'} = \mathscr{T}_{l'}$.

Example 22. Let us assume E as in Example 21. We have $E;\texttt{emit}\ s \xrightarrow{l_i} \texttt{nothing}$, $1 \leqslant i \leqslant 4$, where

$$l_1 = \langle \{s_1^+, s_2^+\}, \{s_1^+ T, s_2^+ s_3\}, \{s_1^- s_2^- s, s_2^- s_1^- s, s_1^- s_2^+ s, s_2^+ s_1^- s\}, \{T\} \rangle,$$

$$l_2 = \langle \{s_1^+, s_2^-\}, \{s_1^+ T\}, \{s_2^+ s_3, s_1^- s_2^- s, s_2^- s_1^- s, s_1^- s_2^+ s, s_2^+ s_1^- s\}, \{T\} \rangle,$$

$$l_3 = \langle \{s_1^-, s_2^+\}, \{s_2^+ s_3, s_1^- s_2^+ s, s_2^+ s_1^- s\}, \{s_1^+ T, s_1^- s_2^- s, s_2^- s_1^- s\}, 0 \rangle,$$

$$l_4 = \langle \{s_1^-, s_2^-\}, \{s_1^- s_2^- s, s_2^- s_1^- s\}, \{s_1^+ T, s_2^+ s_3, s_1^- s_2^+ s, s_2^+ s_1^- s\}, 0 \rangle.$$

Causality terms $s_1^- s_2^- s$ and $s_2^- s_1^- s$ appear in labels of Example 22 to denote that the absence of both s_1 and s_2 causes the production of s. They highlight that there is no logical order between the testing of s_1 and the testing of s_2.

Note that by Proposition 26 it follows that rules *seq_2* and *seq_3* do not depend on the choice of l'.

Let us consider now the statement `signal` s `in` E `end`, and rule *signal*.

We assume a partial function $loc : \mathscr{S} \times \mathscr{L} \rightharpoonup \mathscr{L}$ which is defined for a signal s and a label l if and only if the following conditions are satisfied:

(1) if $s^+ \in S_l$ then $s \in Em(l) = \{s \in \mathscr{S} \mid \vartheta s \in \mathscr{E}_l\}$;
(2) if $s \in Em(l)$ then $s^- \notin S_l$;
(3) if $s \in Em(l)$ then there exists $\vartheta s \in \mathscr{E}_l$ with $s^+, s^- \notin |\vartheta|$;
(4) if $s \notin Em(l)$ then no ϑs with $|\vartheta| \subseteq S_l \cup \{s^-, s^+\}$ is in $\mathscr{N}_l$.

Condition 1 expresses that if s is present then it must be emitted by E, since s is a local signal and cannot be supplied by the external environment. Condition 2 expresses that if s is emitted by E then no substatement of E requiring the absence of s is executed, since s is fed back to E. Condition 3 expresses that if s is emitted by E then we can deduce that s is present without making assumptions on the status of s. In fact, if $\vartheta s \in \mathscr{E}_l$ and neither $s^+ \in |\vartheta|$ nor $s^- \in |\vartheta|$, then s is present since each input signal $z \neq s$ with $z^+ \in |\vartheta|$ (resp. $z^- \in |\vartheta|$) is present (resp. absent). Condition 4 expresses that if s is not emitted by E then we can deduce that s is absent without making assumptions on the status of s. In fact, if $\vartheta_1 s, \ldots, \vartheta_n s \in \mathscr{N}_l$ and $\gamma_i \in |\vartheta_i| \backslash (S_l \cup \{s^-, s^+\})$, $1 \leqslant i \leqslant n$, then s is absent since, for each $1 \leqslant i \leqslant n$, either an input signals $z_i \neq s$ with $z_i^+ = \gamma_i$ is absent or an input signal $z_i \neq s$ with $z_i^- = \gamma_i$ is present.

If we did not keep track of signal causality arising from discarded branches of statements `present`, then we would not be able to check condition 4.

Example 23. Let us assume $E \equiv \texttt{present}\ s\ \texttt{then}\ \ \texttt{emit}\ s\ \texttt{else emit}\ s\ \texttt{end}$. We have $E \xrightarrow{l_1} \texttt{nothing}$, $E \xrightarrow{l_2} \texttt{nothing}$, with $l_1 = \langle \{s^+\}, \{s^+ s\}, \{s^- s\}, 0 \rangle$ and $l_2 = \langle \{s^-\}, \{s^- s\}, \{s^+ s\}, 0 \rangle$. The function loc is not defined for the pairs (s, l_1) and (s, l_2), which

do not satisfy conditions 3 and 2, respectively. So, no transition having `signal` s `in` E `end` as source state exists.

Let us assume that the conditions above are satisfied and that the causality terms in $\mathscr{E}_l \cup \mathscr{N}_l$ having as action s are $\vartheta_1 s, \ldots, \vartheta_v s$, where $\vartheta_i = \gamma_{i,1} \ldots \gamma_{i,n_i}$, $1 \leqslant i \leqslant v$. Let us consider the label l' such that:

(1) If $s \in Em(l)$, $\vartheta_1 s, \ldots, \vartheta_u s \in \mathscr{E}_l$ and $\vartheta_{u+1} s, \ldots, \vartheta_v s \in \mathscr{N}_l$, then:
- $S_{l'} = S_l \backslash \{s^+\}$;
- $\mathscr{E}_{l'} = \{\vartheta[\vartheta_i/s^+][n/s] \mid \vartheta z \in \mathscr{E}_l, |\vartheta_i| \cap \{s^+\} = \emptyset, 1 \leqslant i \leqslant u\}$;
- $\mathscr{N}_{l'} = \{\vartheta[\vartheta_i/s^+][\gamma_{i_1,1} \ldots \overline{\gamma_{i_1,j_{i_1}}} \ldots \gamma_{i_v,1} \ldots \overline{\gamma_{i_v,j_{i_v}}}/s^-][n/s] \mid \vartheta z \in \mathscr{N}_l, |\vartheta_i| \cap \{s^+, s^-\} = \emptyset, 1 \leqslant i \leqslant v, \gamma_{i_h,j_{i_h}} \notin \{s^+, s^-\}, 1 \leqslant j_{i_h} \leqslant n_{i_h}\} \cup \{\vartheta[\vartheta_i/s^+][n/s] \mid \vartheta z \in \mathscr{E}_l, |\vartheta_i| \cap \{s^+, s^-\} = \emptyset, u+1 \leqslant i \leqslant v\}$;
- $\mathscr{T}_{l'} = \mathscr{T}_l$.

(2) If $s \notin Em(l)$ and $\vartheta_1 s, \ldots, \vartheta_v s \in \mathscr{N}_l$, then:
- $S_{l'} = S_l \backslash \{s^-\}$;
- $\mathscr{E}_{l'} = \{\vartheta[\gamma_{i_1,1} \ldots \overline{\gamma_{i_1,j_{i_1}}} \ldots \gamma_{i_v,1} \ldots \overline{\gamma_{i_v,j_{i_v}}}/s^-]z \mid \vartheta z \in \mathscr{E}_l, \{\gamma_{i_h,1}, \ldots, \overline{\gamma_{i_h,j_{i_h}}}\} \subseteq S_l$ and $\gamma_{i_h,j_{i_h}} \notin \{s^+, s^-\}$ for every $1 \leqslant h \leqslant v\}$;
- $\mathscr{N}_{l'} = \{\vartheta[\vartheta_i/s^+][\gamma_{i_1,1} \ldots \overline{\gamma_{i_1,j_{i_1}}} \ldots \gamma_{i_v,1} \ldots \overline{\gamma_{i_v,j_{i_v}}}/s^-][n/s] \mid \vartheta z \in \mathscr{N}_l, |\vartheta_i| \cap \{s^+, s^-\} = \emptyset, 1 \leqslant i \leqslant v, \gamma_{i_h,j_{i_h}} \notin \{s^+, s^-\}, 1 \leqslant j_{i_h} \leqslant n_{i_h}\} \cup \{\vartheta[\gamma_{i_1,1} \ldots \overline{\gamma_{i_1,j_{i_1}}} \ldots \gamma_{i_v,1} \ldots \overline{\gamma_{i_v,j_{i_v}}}/s^-]z \mid \vartheta z \in \mathscr{E}_l, \{\gamma_{i_h,1}, \ldots, \overline{\gamma_{i_h,j_{i_h}}}\} \notin S_l$ for some $1 \leqslant h \leqslant v$ and $\gamma_{i_h,j_{i_h}} \notin \{s^+, s^-\}$ for every $1 \leqslant h \leqslant v\}$;
- $\mathscr{T}_{l'} = \mathscr{T}_l$.

Let consider the first of the two cases, namely let us assume that $s \in Em(l)$.

Since s^+ refers to the signal s local to `signal` s `in` E `end`, we have $S_{l'} = S_l \backslash \{s^+\}$.

Given $\vartheta s \in \mathscr{E}_l \cup \mathscr{N}_l$, we replace s by n, since s cannot be viewed by the external environment. So, the action of producing s by a statement in the body of E corresponds to the action of termination of this statement in the body of `signal` s `in` E `end`.

Since the presence of s is caused by any event ϑ_i such that $|\vartheta_i| \cap \{s^+\} = \emptyset$, $1 \leqslant i \leqslant u$, and could be caused by any event ϑ_i such that $|\vartheta_i| \cap \{s^+, s^-\} = \emptyset$, $u+1 \leqslant i \leqslant v$, then, if $\vartheta z \in \mathscr{E}_l$ and s^+ occurs in ϑ, we have that $\{\vartheta[\vartheta_i/s^+]z[n/s] \mid |\vartheta_i| \cap \{s^+\} = \emptyset, 1 \leqslant i \leqslant u\} \subseteq \mathscr{E}_{l'}$ and $\{\vartheta[\vartheta_i/s^+]z[n/s] \mid |\vartheta_i| \cap \{s^+, s^-\} = \emptyset, u+1 \leqslant i \leqslant v\} \subseteq \mathscr{N}_{l'}$. Analogously, if $\vartheta z \in \mathscr{N}_l$ and s^+ occurs in ϑ, then we have that $\{\vartheta[\vartheta_i/s^+]z[n/s] \mid |\vartheta_i| \cap \{s^+, s^-\} = \emptyset, 1 \leqslant i \leqslant v\} \subseteq \mathscr{N}_{l'}$.

By condition 2 of the definition of $loc(s,l)$, we cannot have a causality term $\vartheta z \in \mathscr{E}_l$ such that s^- occurs in ϑ. If $\vartheta z \in \mathscr{N}_l$ and s^- occurs in ϑ, then we have that $\{\vartheta[\gamma_{i_1,1} \ldots \overline{\gamma_{i_1,j_{i_1}}} \ldots \gamma_{i_v,1} \ldots \overline{\gamma_{i_v,j_{i_v}}}\}/s^-][n/s] \mid \gamma_{i_h,j_{i_h}} \notin \{s^+, s^-\}, 1 \leqslant j_{i_h} \leqslant n_{i_h}\} \subseteq \mathscr{N}_{l'}$. The reason is that if, for each $1 \leqslant i \leqslant v$, signals have not the status assumed by ϑ_i then s is not emitted.

We have $\mathscr{T}_l = \mathscr{T}_{l'}$ since `signal` s `in` E `end` terminates as E does.

The case with $s \notin Em(l)$ is analogous.

Now, since causality terms of the form $\vartheta\mu$ with $\mu = s$ have been replaced by causality terms of the form ϕn, it may happen that a pair of causality terms $\vartheta_1\vartheta_2 n$ and $\vartheta_1 p$ are in $\mathscr{E}_{l'} \cup \mathscr{N}_{l'}$. To remove this redundant information (thus obtaining a coarser notion of

bisimulation), we consider the label $l''=l'\otimes l'$. Now, if $\vartheta z^- n\in\mathscr{E}_{l''}$ then we remove it and we add $\vartheta z^+ n$ to $\mathscr{N}_{l''}$, since $\vartheta z^- n$ cannot appear in any label. Analogously, if $\vartheta z^- n\in\mathscr{N}_{l''}$ then we remove it and we add $\vartheta z^+ n$ to either $\mathscr{E}_{l''}$, if $|\vartheta|\cup\{z^+\}\subseteq S_{l''}$, or to $\mathscr{N}_{l''}$, otherwise. Then, we consider the label thus obtained as $loc(s,l)$.

Example 24. Let us assume $E\equiv$ `signal` s_2 `in` $E_1 \parallel E_2$ `end`, where
$E_1\equiv$ `present` s_1 `then emit` s_2 `else nothing end`,
$E_2\equiv$ `present` s_2 `then emit` s_3 `else nothing end`.
By rule signal we have $E\xrightarrow{l_1}$ `signal` s_2 `in (nothing` $\parallel$ `nothing) end` and $E\xrightarrow{l_2}$ `signal` s_2 `in (nothing` $\parallel$ `nothing) end`, where $l_1=\langle\{s_1^+\},\{s_1^+ s_3\},\emptyset,0\rangle$ and $l_2=\langle\{s_1^-\},\emptyset,\{s_1^+ s_3\},0\rangle$.

Note that we have $E\approx$ `present` s_1 `then emit` s_3 `else nothing end`.

Let us consider now the statement `trap` T `in` E `end`.

Given a transition $E\xrightarrow{l}F$ with $\vartheta_1 T,\ldots,\vartheta_n T$ the causality terms in $\mathscr{E}_l\cup\mathscr{N}_l$ having T as action, $\vartheta_i=\gamma_{i,1}\ldots\gamma_{i,n_i}$, we denote with $T(l)$ the set of ordered events $\gamma_{i_1,1}\ldots\overline{\gamma_{i_1,j_{i_1}}}\ldots\gamma_{i_n,1}\ldots\overline{\gamma_{i_n,j_{i_n}}}$, where $1\leqslant j_{i_h}\leqslant n_{i_h}$ for $1\leqslant h\leqslant n$. Given an ordered event $\phi\in T(l)$, if each signal s with $s^+\in|\phi|$ is present and each signal s with $s^-\in|\phi|$ is absent, then E does not exit the trap T, since no statement `exit` T is executed.

Now, given a label l and a trap name T, let l' be the label such that:

- $S_{l'}=S_l$;
- $\mathscr{E}_{l'}=\mathscr{E}_l[\{\phi\vartheta p\mid\phi\in T(l),|\phi|\uparrow S_l,|\vartheta|\uparrow|\vartheta_i|$ for some $1\leqslant i\leqslant n\}/\vartheta p][\vartheta n/\vartheta T]$;
- $\mathscr{N}_{l'}=\mathscr{N}_l[\{\phi\vartheta p\mid\phi\in T(l),|\vartheta|\uparrow|\vartheta_i|$ for some $1\leqslant i\leqslant n\}/\vartheta p][\vartheta n/\vartheta T]\cup\{\phi\vartheta p\mid\phi\in T(l),|\phi|\not\uparrow S_l,|\vartheta|\uparrow|\vartheta_i|$ for some $1\leqslant i\leqslant n,\vartheta p\in\mathscr{E}_l\}$;
- $$\mathscr{T}_{l'}=\begin{cases}1 & \text{if } \mathscr{T}_l=1,\\ 0 & \text{if } \mathscr{T}_l=0 \text{ or } \mathscr{T}_l=\{T\},\\ \mathscr{T}_l\backslash\{T\} & \text{otherwise.}\end{cases}$$

If $\mathscr{T}_l=1$ then $\mathscr{T}_{l'}=1$, since `trap` T `in` E `end` pauses whenever E pauses. If $\mathscr{T}_l=0$ or $\mathscr{T}_l=\{T\}$ then $\mathscr{T}_{l'}=0$, since `trap` T `in` E `end` terminates whenever E either terminates or exits the trap T. If $\mathscr{T}_l\subseteq\mathscr{T}$ and $\mathscr{T}_l\neq\{T\}$ then $\mathscr{T}_{l'}=\mathscr{T}_l\backslash\{T\}$, since `trap` T `in` E `end` exits a trap $T'\neq T$ when E exits T'.

If there exists a causality term $\vartheta p\in\mathscr{E}_l$ with $|\vartheta|\uparrow|\vartheta_i|$ for some $1\leqslant i\leqslant n$, then we replace it by the set of causality terms of the form $\phi\vartheta p$, where $\phi\in T(l)$ and $\phi\uparrow S_l$, since the whole statement pauses only if E does not exit the trap T. Causality terms of the form $\phi\vartheta p$, where $\phi\in T(l)$ and $|\phi|\not\uparrow S_l$, are added to $\mathscr{N}_{l'}$. Analogously, we replace a causality term ϑp in $\mathscr{N}_l$ such that $|\vartheta|\uparrow|\vartheta_i|$ for some $1\leqslant i\leqslant n$ by the set of causality terms of the form $\phi\vartheta p$, with $\phi\in T(l)$.

Causality terms of the form ϑT in $\mathscr{E}_l\cup\mathscr{N}_l$ are replaced by ϑn, since the action of exiting T by a statement in the body of E corresponds to the action of termination of this statement in the body of `trap` T `in` E `end`.

Now, since causality terms of the form ϑT have been replaced by causality terms of the form ϑn, it may happen that a pair of causality terms $\vartheta_1\vartheta_2 n$ and $\vartheta_1 p$ are in $\mathscr{E}_{l'} \cup \mathscr{N}_{l'}$. To remove this redundant information, we consider the label $l'' = l' \otimes l'$. Now, if $\vartheta s^- n \in \mathscr{E}_{l''}$ then we remove it and we add $\vartheta s^+ n$ to $\mathscr{N}_{l''}$, since $\vartheta s^- n$ cannot appear in any label. Analogously, if $\vartheta s^- n \in \mathscr{N}_{l''}$ then we remove it and we add $\vartheta s^+ n$ to either $\mathscr{E}_{l''}$, if $|\vartheta| \cup \{s^+\} \subseteq S_{l''}$, or to $\mathscr{N}_{l''}$, otherwise. Then, we consider the label thus obtained as $tr(T, l)$.

Example 25. Let $E \equiv E_1 \parallel E_2$, where
$E_1 \equiv$ `present` s_1 `then pause else nothing end`,
$E_2 \equiv$ `present` s_2 `then exit` T `else nothing end`.
By rules trap_1, trap_2, trap_3, we have `trap` T `in` E `end` $\xrightarrow{l_i}$, $1 \leqslant i \leqslant 4$, where

$$l_1 = \langle \{s_1^+, s_2^+\}, \emptyset, \{s_2^- s_1^+ p\}, 0\rangle\}, \quad l_2 = \langle \{s_1^+, s_2^-\}, \{s_2^- s_1^+ p\}, \emptyset, 1\rangle\},$$

$$l_3 = \langle \{s_1^-, s_2^+\}, \emptyset, \{s_2^- s_1^+ p\}, 0\rangle\}, \quad l_4 = \langle \{s_1^-, s_2^-\}, \emptyset, \{s_2^- s_1^+ p\}, 0\rangle\}.$$

We can prove now some properties of the LTS.

The following proposition states that labels of transitions departing from a given LTS state contain the same set of causality terms.

Proposition 26. *Given a statement E and transitions $E \xrightarrow{l_1} F_1$, $E \xrightarrow{l_2} F_2$, it holds that $\mathscr{E}_{l_1} \cup \mathscr{N}_{l_1} = \mathscr{E}_{l_2} \cup \mathscr{N}_{l_2}$.*

Proof. By structural induction over E. □

The following proposition states that two arbitrary LTS transitions having a statement E as source state represent reactions of E to different inputs from the environment.

Proposition 27. *If $E \xrightarrow{l_1} F_1$ and $E \xrightarrow{l_2} F_2$ then $S_{l_1} \not\asymp S_{l_2}$.*

Proof. By structural induction on E.

Base case: If E is a basic statement then exactly one transition has E as source state and the thesis is immediate.

Induction step: Let us assume that $E \equiv$ `present` s `then` E_1 `else` E_2 `end`. If both $E \xrightarrow{l_1} F_1$ and $E \xrightarrow{l_2} F_2$ represent reactions of E_1 (resp. E_2) then the thesis follows by inductive hypothesis on E_1 (resp. E_2) and by the definition of $s^+(l, l')$ (resp. $s^-(l', l)$). If $E \xrightarrow{l_1} F_1$ represents a reaction of E_1 and $E \xrightarrow{l_2} F_2$ represents a reaction of E_2 then the thesis follows by the fact that $s^+ \in S_{l_1}$ and $s^- \in S_{l_2}$.

In the other cases the thesis follows directly by the inductive hypothesis. □

We say that a consistent event S_I is an *input event* if it is an assumption over all input signals, namely either $i^+ \in S_I$ or $i^- \in S_I$ for every i in the set of input signals I.

We introduce now a notion of constructiveness of statements.

Definition 28. A *statement* E is *constructive* if for each input event S_I there exists a transition $E \xrightarrow{I} F$ such that $S_I \uparrow S_I$.

Nonconstructiveness may arise when applying rule *signal*, if the status of the local signal s cannot be determined without making any assumption on it.

Example 29. The statement `signal` s `in` E `end`, where
$E \equiv$ `present` s `then emit` s `else emit` s `end`
as in Example 23, is nonconstructive, since no transition has it as source state.

A statement constructive as in Definition 28 is reactive and deterministic. The reactivity follows by the fact that a reaction exists for every input event. The determinism follows by Proposition 27.

3.3. A comparison with existing LTSs for Esterel

As it is explained in [31], attempts to give semantics for Esterel in terms of synchronous process calculi, such as Milner's SCCS and Austry and Boudol's Meije, were not successful. We believe that the reason is that, as it is explained in [10], SCCS and Meije are somewhat weaker than Esterel, since they do not offer primitives to instantaneously test the absence of signals.

By adopting Plotkin's structural operational semantics, semantics for Esterel in terms of LTSs have been successfully proposed in [12, 14, 11]. In this subsection we compare these approaches with our.

The semantics of [11] considers LTS transitions of the form $E \xrightarrow{\langle S_i, S_o, k\rangle} E'$, where S_i is a consistent event over the set of input signals I, S_o is a set of output signals in O, and k is an integer giving information on the termination of E. So, labels considered in [11] do not carry any information on signal causality, which, on the contrary, appears in our LTS labels and has been exploited in rule *signal* to determine the behavior of `signal` s `in` E `end`. More precisely, we have exploited information on signal causality to determine whether label $loc(s, l)$ is defined or not, i.e. whether the status of s can be determined without making any assumption on it. In [11], transitions having `signal` s `in` E `end` as source state are inferred from transitions $E \xrightarrow{\langle S_i, S_o, k\rangle} E'$ and from the value of two sets of signals $Must(E, S_i)$ and $Cannot(E, S_i)$. Now, a signal s is in $Must(E, S_i)$ (resp. $Cannot(E, S_i)$) if one can infer that s is present (resp. absent) from the information given by S_i without making any assumption on s. A reaction of `signal` s `in` E `end` is inferred from a transition $E \xrightarrow{\langle S_i, S_o, k\rangle} E'$ if either $s \in Must(E, S_i)$ or $s \in Cannot(E, S_i)$. The sets $Must(E, S_i)$ and $Cannot(E, S_i)$ are constructed compositionally w.r.to the structure of E, by exploiting information on signal causality analogous to that carried by our labels. So, we use the same information used in [11] to determine the behavior of `signal` s `in` E `end`. The difference is that we explicitly represent it on labels.

From the correspondence between our LTS interpretation and the circuit semantics (see Section 5), and from the correspondence between the LTS interpretation of [11] and the circuit semantics (see [11]), it follows that the two LTS interpretations agree. More precisely, we infer $E \xrightarrow{l} E'$ from rules in Table 1 if and only if transition $E \xrightarrow{\langle S_i, S_o, k\rangle} E'$ is inferred in [11], where $S_l = S_i$, $Em(l) = S_o$, $k = 0$ iff $\mathscr{T}_l = 0$, $k = 1$ iff $\mathscr{T}_l = 1$ and $k = i$ iff E exits T, $T \in \mathscr{T}_l$ and T is the ith outermost trap.

Given statements E and F, we consider E and F as equivalent iff they are bisimilar according to our LTS semantics. If one considers the LTS semantics of [11], it is reasonable to consider E and F as equivalent iff they are bisimilar, $Must(E, S_i) = Must(F, S_i)$, and $Cannot(E, S_i) = Cannot(F, S_i)$, for every input event S_i. It is not sufficient that E and F are bisimilar, since, if $E \approx F$ but either $Must(E, S_i) \neq Must(F, S_i)$ or $Cannot(E, S_i) \neq Cannot(F, S_i)$, then, in general, we are not sure that `signal` s `in` E `end` $\approx$ `signal` s`in` F `end`.

So, the main difference between our LTS and the LTS in [11] is that we explicitly represent information on signal causality in our label. On one side, our choice make the LTS heavy, but, on the other side, it is easier to prove the property of congruence of our equivalence, because we need only to prove that bisimulation is a congruence, and this fact follows immediately from the format of the SOS rules.

The LTS semantics of [12, 14] deal with the nonconstructive version of the language, in the sense that all reactive and deterministic statements are accepted, even if they are nonconstructive. So, sets $Must(E, S_i)$ and $Cannot(E, S_i)$ are not considered in [12, 14].

4. The axiomatization

In this section we introduce the process algebra Esterel$^+$, which strictly contains the terms of the process algebra Esterel, and we give a TSS for Esterel$^+$ that is an operational conservative extension (cf. Definition 9) of the TSS for Esterel. In Section 4.1, we provide an axiomatization over Esterel$^+$ and we prove that it is sound modulo bisimulation. Since the TSS for Esterel$^+$ is an operational conservative extension of the TSS for Esterel, the axiomatization is also sound modulo bisimulation over Esterel. In Section 4.2, we prove that our axiomatization is complete modulo bisimulation on constructive Esterel statements.

The choice of giving an axiomatization for a superset of a given language is well-established in the literature. As an example, in [26] it is proved that process algebras offering operations of nondeterministic choice, prefixing and merge can be finitely axiomatized modulo bisimulation only by extending the original signature. In [6] it is shown how a finite axiomatization can be given by adding to the original signature the "left merge" operation.

In [2] an algorithm is given to construct from a *GSOS language* L [13] both a superset L' of L and a finite unconditional axiomatization $\mathscr{A}$ such that $\mathscr{A}$ and the "approximation induction principle" (AIP) [7, 16] together are sound and complete

modulo bisimulation on L'. AIP is an infinitary conditional axiom which states that two processes are equated provided that all their finite projections are. In general, one is interested in avoiding infinitary axioms like AIP. In [1] an algorithm is given to construct from a *regular GSOS language* L [1] both a superset L' of L and a finite unconditional axiomatization $\mathscr{A}$ such that $\mathscr{A}$, the "recursive definition principle" (RDP) and the "recursion specification principle" (RSP) [24, 8] together are sound and complete modulo bisimulation on L'.

We cannot exploit here the results of [2, 1]. In these papers, process algebras offering the operation of summation "+" and the operation of prefixing "·" are considered. Prefixing permits to prefix a process p by an action a, where a is an action observable by the external world, namely an action that may be a label of the LTS. Summation denotes the nondeterministic choice. In [2, 1], like in [24], the idea is to have axioms such that, for a given process p, one can infer $p = \sum_{i\in I} a_i \cdot p_i$. Namely, the idea is to transform every process into a "head normal form". A concurrent process $p_1 \parallel p_2$ can be transformed into a head normal form because p_1 and p_2 are not synchronized and the concurrency of their actions is simulated by arbitrary interleaving. We cannot have head normal forms for Esterel. In fact, we cannot transform a concurrent statement into a sequential one because concurrent statements are perfectly synchronized. We will introduce therefore normal forms admitting the construct "$\|$".

So, we propose a countably infinite axiomatization over Esterel$^+$ which is sound and complete modulo bisimulation on Esterel. All axioms are finitary, and all axioms except RSP are unconditional.

Let us assume a set of *recursion variables Var* ranged over by P. The terms (statements) of the algebra Esterel$^+$ are those generated by the following BNF-like grammar:

$$\begin{aligned} E ::= {} & \texttt{nothing} \mid \texttt{emit}\ s \mid \texttt{pause} \mid \texttt{present}\ s\ \texttt{then}\ E\ \texttt{else}\ E\ \texttt{end} \mid E \parallel E \mid \\ & E\ ;\ E \mid \texttt{signal}\ s\ \texttt{in}\ E\ \texttt{end} \mid \texttt{loop}\ E\ \texttt{end} \mid \texttt{suspend}\ E\ \texttt{when}\ s \mid \\ & \texttt{trap}\ T\ \texttt{in}\ E\ \texttt{end} \mid \texttt{exit}\ T \mid \texttt{rec}\ P.E \mid P \end{aligned}$$

where s, T and P range over $\mathscr{S}$, $\mathscr{T}$ and *Var*, respectively.

Construct `rec` is analogous to recursion constructs of most of the process algebras. Its operational semantics is defined by the following transition rule:

$$\frac{E[\texttt{rec}\ P.E/P] \xrightarrow{l} F}{\texttt{rec}\ P.E \xrightarrow{l} F}\ (rec).$$

Construct `rec` permits to simulate behaviors that can be defined by combining construct `loop` and mechanism `trap-exit`.

Example 30. Let us assume the Esterel$^+$ statements E_1 and E_2 such that
$E_1 \equiv \texttt{rec}\ P.\texttt{present}\ s\ \texttt{then}\ (\texttt{pause}; P)\ \texttt{else}\ \texttt{nothing}\ \texttt{end}$,
$E_2 \equiv \texttt{trap}\ T\ \texttt{in}\ (\texttt{loop}\ (\texttt{present}\ s\ \texttt{then}\ \texttt{pause}\ \texttt{else}\ \texttt{exit}\ T\ \texttt{end})\ \texttt{end})\ \texttt{end}$.

We have $E_1 \approx E_2$. In fact, $E_1 \xrightarrow{l} \texttt{nothing}; E_1$, $E_1 \xrightarrow{l'} \texttt{nothing}$, $E_2 \xrightarrow{l} \texttt{trap}\ T\ \texttt{in}\ (\texttt{nothing}; \texttt{loop}(\texttt{present}\ s\ \texttt{then}\ \texttt{pause}\ \texttt{else}\ \texttt{exit}\ T\ \texttt{end})\ \texttt{end})\ \texttt{end}$,

Table 2

Axioms for "$\|$".			
$E \,\|\, F = F \,\|\, E$	$(\|_1)$	$E \,\|\, \texttt{nothing} = E$	$(\|_3)$
$E \,\|\, (F \,\|\, G) = (E \,\|\, F) \,\|\, G$	$(\|_2)$	$E \,\|\, E = E$	$(\|_4)$

Table 3

Axioms for present_then_else_end.	
$\texttt{present}\ s\ \texttt{then}\ E\ \texttt{else}\ F\ \texttt{end} = \texttt{if}\ s^+\ \texttt{then}\ E \,\|\, \texttt{if}\ s^-\ \texttt{then}\ F$	$(?_1)$
$\texttt{if}\ s^+\ \texttt{then}\ (E \,\|\, F) = \texttt{if}\ s^+\ \texttt{then}\ E \,\|\, \texttt{if}\ s^+\ \texttt{then}\ F$	$(?_2)$
$\texttt{if}\ s^-\ \texttt{then}\ (E \,\|\, F) = \texttt{if}\ s^-\ \texttt{then}\ E \,\|\, \texttt{if}\ s^-\ \texttt{then}\ F$	$(?_3)$

$E_2 \xrightarrow{l'} \texttt{nothing}$, where $l = \langle \{s^+\}, \{s^+ p\}, \emptyset, 1\rangle$ and $l' = \langle \{s^-\}, \emptyset, \{s^+ p\}, 0\rangle$, and, in general, $E \approx \texttt{nothing}; E$ for any E.

Proposition 31. *The TSS for Esterel$^+$ is an operational conservative extension of the TSS for Esterel.*

Proof. All transition rules in Table 1 are source dependent (cf. Definition 10) and the source of rule *rec* contains the operator rec, which is not an Esterel operator. So, the requirements of Theorem 11 are fulfilled and the thesis follows. □

Given a statement E, we say that an occurrence of a variable $P \in Var$ is *free* in E if it does not appear in any statement $\texttt{rec}\, P.F$ in the body of E.

A variable P is free in E if an occurrence of P is free in E. The set of variables free in E is denoted with $Free(E)$.

A variable P is *guarded* in E if each free occurrence of P in E appears in a subexpression $F; P$ such that F cannot terminate immediately.

Intuitively, if we consider a statement $\texttt{rec}\, P.E$ with P free in E, then we are sure that if P is guarded in E then every reaction of $\texttt{rec}\, P.E$ is finite. As an example, let us consider statements $E_1 \equiv \texttt{pause}; P$ and $E_2 \equiv \texttt{emit}\, s; P$. Variable P is guarded in E_1 but not in E_2. Now, $\texttt{rec}\, P.E_1$ performs a statement pause at each execution cycle, while $\texttt{rec}\, P.E_2$ executes $\texttt{emit}\, s$ infinitely many times at the first execution cycle.

4.1. The axioms

We consider the axiomatization over Esterel$^+$ given by axioms in Tables 2–8.

Axioms $\|_1$, $\|_2$ and $\|_3$ in Table 2 state that construct $\|$ is commutative and associative and has nothing as neutral element. Axiom $\|_2$ allows to denote with $E \,\|\, F \,\|\, G$ both statements $E \,\|\, (F \,\|\, G)$ and $(E \,\|\, F) \,\|\, G$. Axiom $\|_4$ follows by the fact that every statement E is deterministic and by the fact that statements running in parallel are perfectly synchronized.

Proposition 32. *The axioms in Table 2 are sound modulo bisimulation.*

Table 4

Other axioms for "‖".

$s^-, s^+ \notin \lvert\vartheta\rvert \Rightarrow$	`if` ϑ `then pause;` E	$=$	`if`	ϑ	`then pause`	$(\|\|_5)$
				‖		
			`if`	ϑs^+	`then pause;` E	
				‖		
			`if`	ϑs^-	`then pause;` E	
$\gamma \notin \lvert\vartheta\rvert \Rightarrow$	`if` ϑ `then pause`	$=$	`if`	ϑ	`then pause`	$(\|\|_6)$
				‖		
			`if`	$\vartheta\gamma$	`then pause`	
$\lvert\vartheta\rvert = \lvert\vartheta'\rvert \Rightarrow$	`if` ϑ `then pause;` E	$=$	`if`	ϑ	`then pause;` $(E \,\|\|\, F)$	$(\|\|_7)$
	‖			‖		
	`if` ϑ' `then pause;` F		`if`	ϑ'	`then pause`	
$\lvert\vartheta\rvert \subseteq \lvert\vartheta'\rvert \Rightarrow$	`if` ϑ `then exit` T	$=$	`if`	ϑ	`then exit` T	$(\|\|_8)$
	‖			‖		
	`if` ϑ' `then pause;` E		`if`	ϑ'	`then pause`	
$\gamma \notin \lvert\vartheta\rvert \Rightarrow$	`if` ϑ `then pause`	$=$	`if`	ϑ	`then pause`	$(\|\|_9)$
				‖		
			`if`	$\vartheta\gamma$	`then nothing`	

Table 5

Axioms for `rec` and `loop_end`.

	$\texttt{rec}\, P.E = E\,[\texttt{rec}\, P.E/P]$	(rec_1)
P guarded in $E, F = E[F/P] \Rightarrow$	$F = \texttt{rec}\, P.E$	(rec_2)
	$\texttt{loop}\ E\ \texttt{end} = \texttt{rec}\, P.(E; P)$	$(loop_1)$

Table 6

Axioms for ";".

	$E; (F \,\|\|\, G) = (E; F) \,\|\|\, (E; G)$	(seq_1)
E normal form and $Free(E) = \emptyset \Rightarrow$	$E; H = E^H$	(seq_2)
	$\texttt{pause}; \texttt{nothing} = \texttt{pause}$	(seq_3)

Table 7

Axioms for `suspend _ when _` and `trap _ in _ end`.

E normal form and $Free(E) = \emptyset \Rightarrow$ `suspend` E `when` $s = E^s$ $(susp)$

E normal form and $Free(E) = \emptyset \Rightarrow$ `trap` T `in` E `end` $= E^T$ $(trap)$

Table 8

Axioms for `signal _ in _ end`.

`signal` s `in (signal` s `in` E `end) end = signal` s `in` E `end` (s_1)

E normal form and $Free(E) = \emptyset \Rightarrow$

`signal` s `in` E `end = signal` s `in` E_s `end` (s_2)

E normal form, E constructive and $Free(E) = \emptyset \Rightarrow$

`signal` s `in` E_s `end` $= E \backslash \{s\}$ (s_3)

Proof. The thesis follows by the fact that $\otimes$ is commutative and associative (see Propositions 19–20), has δ as neutral element, and is such that $l \otimes l = l$ for every label l constructed by means of rules in Table 1. □

Let us introduce now some notations.
Assume a signal $s \in \mathscr{S}$, an ordered event $\vartheta \in (\mathscr{S}^{+}_{-})^{*}$, and a statement E.
We write $\texttt{if } s^{+} \texttt{ then } E$ for $\texttt{present } s \texttt{ then } E \texttt{ else nothing end}$.
We write $\texttt{if } s^{-} \texttt{ then } E$ for $\texttt{present } s \texttt{ then nothing else } E \texttt{ end}$.
We write

$$\texttt{if } \vartheta \texttt{ then } E \text{ for } \begin{cases} E & \text{if } \vartheta = \varepsilon, \\ \texttt{if } \gamma \texttt{ then if } \phi \texttt{ then } E & \text{if } \vartheta = \gamma\phi. \end{cases}$$

Axiom $?_1$ in Table 3 is justified by the fact that, in both statements, E is executed if s is present, whereas F is executed if s is absent.

Axiom $?_2$ is justified by the fact that both E and F are executed if and only if s is present. Axiom $?_3$ is analogous.

Proposition 33. *The axioms in Table* 3 *are sound modulo bisimulation.*

Proof. To prove the soundness of axiom $?_1$, let us consider statements $H \equiv \texttt{present } s \texttt{ then } E \texttt{ else } F \texttt{ end}$ and $H' \equiv \texttt{if } s^{+} \texttt{ then } E \parallel \texttt{if } s^{-} \texttt{ then } F$, and let us assume that $E \xrightarrow{l_1} E'$ and $F \xrightarrow{l_2} F'$.

We have $H \xrightarrow{s^{+}(l_1,l_2)} E'$. Now, $E \xrightarrow{l_1} E'$ iff $\texttt{if } s^{+} \texttt{ then } E \xrightarrow{l'_1} E'$, where $l'_1 = s^{+}(l_1, \delta)$. Moreover, $F \xrightarrow{l_2} F'$ iff $\texttt{if } s^{-} \texttt{ then } F \xrightarrow{l'_2} \texttt{nothing}$, where $l'_2 = s^{+}(\delta, l_2)$. So, we have $H' \xrightarrow{l'_1 \otimes l'_2} E' \parallel \texttt{nothing}$, where $l'_1 \otimes l'_2 = s^{+}(l_1, l_2)$ and, by axioms in Table 2, $E' \approx E' \parallel \texttt{nothing}$.

Analogously, we have $H \xrightarrow{l} F'$ iff $H' \xrightarrow{l} \texttt{nothing} \parallel F'$, $l = s^{-}(l_2, l_1)$, and, therefore, $H \approx H'$.

Let us consider now axiom $?_2$ and statements $H \equiv \texttt{if } s^{+} \texttt{ then } (E \parallel F)$ and $H' \equiv \texttt{if } s^{+} \texttt{ then } E \parallel \texttt{if } s^{+} \texttt{ then } F$.

We have $H \xrightarrow{l} E' \parallel F'$ iff $E \xrightarrow{l_1} E'$, $F \xrightarrow{l_2} F'$ and $l = s^{+}(l_1 \otimes l_2, \delta)$. Now, $E \xrightarrow{l_1} E'$ and $F \xrightarrow{l_2} F'$ iff $H' \xrightarrow{l'} E' \parallel F'$, where $l' = s^{+}(l_1, \delta) \otimes s^{+}(l_2, \delta)$. Note that $l = l'$.

Moreover, we have $H \xrightarrow{l} \texttt{nothing}$ iff $E \xrightarrow{l_1} E'$, $F \xrightarrow{l_2} F'$, $l = s^{-}(\delta, l_1 \otimes l_2)$. Now, $E \xrightarrow{l_1} E'$, $F \xrightarrow{l_2} F'$ iff $H' \xrightarrow{l'} \texttt{nothing} \parallel \texttt{nothing}$, $l' = s^{-}(\delta, l_1) \otimes s^{-}(\delta, l_2)$. Note that $l = l'$, and, by axiom $\parallel_3$, $\texttt{nothing} \approx \texttt{nothing} \parallel \texttt{nothing}$.

So, it follows that $H \approx H'$.

The soundness of axiom $?_3$ can be proved analogously. □

Axiom $\parallel_5$ in Table 4 is justified by the fact that the statement on the right side of "=" pauses, independently of the status of signal s, if the environment prompts every signal z such that $z^{+} \in |\vartheta|$ and does not prompt any signal z such that $z^{-} \in |\vartheta|$.

Moreover, in this case, both statements will behave as E at the next execution cycle. Note that we could not have an analogous axiom with an arbitrary statement replacing pause; E. As an example, we could not have $H = H'$, for $H \equiv$ emit z and $H' \equiv$ emit $z \parallel$ if s^+ then emit $z \parallel$ if s^- then emit z. In fact, H' terminates only when the status of signal s is known. So, signal s,z in (H; if z then emit s) end is constructive, while signal s,z in (H'; if z then emit s) end is nonconstructive.

Axiom $\|_6$ is justified by the fact that, if the environment prompts every signal z such that $z^+ \in |\vartheta|$ and does not prompt any signal z such that $z^- \in |\vartheta|$, then the statement on the right side of "=" pauses independently of the status of the signal s such that $\gamma \in \{s^+, s^-\}$.

Axiom $\|_7$ is justified by the fact that in both statements, E and F start in the same cycle and run concurrently.

Axiom $\|_8$ is justified by the fact that both statements cannot pause.

Axiom $\|_9$ is justified by the fact that, if the environment prompts every signal z such that $z^+ \in |\vartheta|$ and does not prompt any signal z such that $z^- \in |\vartheta|$, then the statement in the right side of "=" pauses independently of the status of the signal s such that $\gamma \in \{s^+, s^-\}$.

Proposition 34. *The axioms in Table* 4 *are sound modulo bisimulation.*

Proof. To prove the soundness of axiom $\|_5$, let us consider statements $H \equiv$ if ϑ then pause; E and $H' \equiv$ if ϑ then pause $\parallel$ if ϑs^+ then pause; $E \parallel$ if ϑs^- then pause; E.

We have $H \xrightarrow{l}$ nothing; E iff, either $H' \xrightarrow{l_1}$ nothing $\parallel$ (nothing; E) $\parallel$ nothing or $H' \xrightarrow{l_2}$ nothing $\parallel$ nothing $\parallel$ (nothing; E), where l, l_1 and l_2 are the labels such that $l = \langle |\vartheta|, \{\vartheta p\}, \emptyset, 1\rangle$,

$l_1 = l \otimes \langle |\vartheta| \cup \{s^+\}, \{\vartheta s^+ p\}, \emptyset, 1\rangle \otimes \langle |\vartheta| \cup \{s^+\}, \emptyset, \{\vartheta s^- p\}, 0\rangle$ and

$l_2 = l \otimes \langle |\vartheta| \cup \{s^-\}, \emptyset, \{\vartheta s^+ p\}, 0\rangle \otimes \langle |\vartheta| \cup \{s^-\}, \{\vartheta s^- p\}, \emptyset, 1\rangle$.

Now, $l = l_1$. In fact, $\vartheta s^+ p \notin \mathscr{E}_{l_1}$ and $\vartheta s^- p \notin \mathscr{N}_{l_1}$ since $\vartheta p \in \mathscr{E}_{l_1}$, and $s^+ \notin S_{l_1}$. Analogously, $l = l_2$. Moreover, by axiom $\|_3$, we have that

nothing; $E \approx$ nothing $\parallel$ (nothing; E) $\parallel$ nothing and

nothing; $E \approx$ nothing $\parallel$ nothing $\parallel$ (nothing; E).

Let $\vartheta = \gamma_1 \ldots \gamma_n$. We have $H \xrightarrow{l}$ nothing with $l = \langle \{\gamma_1, \ldots, \overline{\gamma_i}\}, \emptyset, \{\vartheta p\}, 0\rangle$ iff $H' \xrightarrow{l'}$ nothing $\parallel$ nothing $\parallel$ nothing with $l' = l \otimes \langle \{\gamma_1, \ldots, \overline{\gamma_i}\}, \emptyset, \{\vartheta s^+ p\}, 0\rangle \otimes \langle \{\gamma_1, \ldots, \overline{\gamma_i}\}, \emptyset, \{\vartheta s^- p\}, 0\rangle$. Now, $l = l'$ and nothing $\approx$ nothing $\parallel$ nothing $\parallel$ nothing.

It follows that $H \approx H'$.

The soundness of axioms $\|_6$ and $\|_9$ can be proved analogously.

To prove the soundness of axiom $\|_7$, let us consider statements

$H \equiv$ if ϑ then pause; $E \parallel$ if ϑ' then pause; F and

$H' \equiv$ if ϑ then pause; ($E \,\|\, F$) $\parallel$ if ϑ' then pause, with $|\vartheta| = |\vartheta'|$.

We have $H \xrightarrow{l}$ nothing $\parallel$ nothing iff $H' \xrightarrow{l}$ nothing $\parallel$ nothing, and

$H \xrightarrow{l}$ nothing; $E \parallel$ nothing; F iff $H' \xrightarrow{l}$(nothing; ($E \,\|\, F$)) $\parallel$ nothing,

where $\texttt{nothing};E \parallel \texttt{nothing};F \approx (\texttt{nothing};(E \parallel F)) \parallel \texttt{nothing}$ by axiom $\parallel_3$ and by the fact that $\texttt{nothing};E \approx E$ for every statement E. So, $H \approx H'$.

To prove the soundness of axiom $\parallel_8$, let us consider statements

$H \equiv \texttt{if } \vartheta \texttt{ then exit } T \parallel \texttt{if } \vartheta' \texttt{ then pause};E$ and

$H' \equiv \texttt{if } \vartheta \texttt{ then exit } T \parallel \texttt{if } \vartheta' \texttt{ then pause}$, with $|\vartheta| \subseteq |\vartheta'|$.

We have $H \xrightarrow{l} \texttt{nothing} \parallel \texttt{nothing}$ with $\mathscr{T}_l = 0$ iff $H' \xrightarrow{l} \texttt{nothing} \parallel \texttt{nothing}$, and $H \xrightarrow{l} \texttt{nothing}$ with $\mathscr{T}_l \subseteq \mathscr{T}$ iff $H' \xrightarrow{l} \texttt{nothing}$. So, $H \approx H'$. □

Axioms rec_1, rec_2 in Table 5 are standard and correspond to RDP and RSP, respectively. Axiom $loop_1$ states that construct `rec` embeds construct `loop`.

Proposition 35. *The axioms in Table 5 are sound modulo bisimulation.*

Proof. The soundness of axiom rec_1 follows directly by transition rule *rec*.

Since rec_1 is sound, to prove the soundness of rec_2 it is sufficient to prove that, for any pair of statements F and G, $F \approx E[F/P]$ and $G \approx E[G/P]$, where P is guarded in E, imply $F \approx G$. To this purpose, let us assume the relation $R = \{(E'[F/P], E'[G/P])\}$ and let us prove that R is a bisimulation.

Since $F \approx E[F/P]$, it holds that $E'[F/P] \xrightarrow{l}$ iff $E'[E[F/P]/P] \xrightarrow{l}$. Analogously, $E'[G/P] \xrightarrow{l}$ iff $E'[E[G/P]/P] \xrightarrow{l}$. Since P is guarded in E, we have $E'[E[F/P]/P] \xrightarrow{l}$ iff $E'[E[G/P]/P] \xrightarrow{l}$. Therefore, $E'[F/P] \xrightarrow{l} H_1$ iff $E'[G/P] \xrightarrow{l} H_2$, for some H_1 and H_2. Note that $H_1 \equiv E''[F/P]$ and $H_2 \equiv E''[G/P]$ for some statement E'', namely $(H_1, H_2) \in R$.

So, we have proved that $R \subseteq \mathscr{F}(R)$, namely that R is a bisimulation. Since $(E[F/P], E[G/P]) \in R$, $F \approx E[F/P]$, and $G \approx E[G/P]$, we have that $F \approx G$.

The soundness of axiom $loop_1$ follows by rules *rec*, *loop_1* and *loop_2*. □

We introduce now a notion of normal form, which will be used to give axioms for constructs ";", `trap`, `suspend` and `signal`.

Definition 36. A statement E is a *normal form* if and only if there exist statements $F_1, \ldots, F_n$, $F_i \not\equiv F_j$, such that:

(1) $E \equiv F_1 \parallel \ldots \parallel F_n$, and, for each $1 \leqslant i \leqslant n$, we have that $F_i \equiv \texttt{if } \vartheta_i \texttt{ then } G_i$, where either $G_i \equiv P$, or G_i is a basic statement, or $|\vartheta_i| \cap \{s^-, s^+\} \neq \emptyset$ for every $s \in \mathscr{S}$ and $G_i \equiv \texttt{pause};E_{f(i)}$;

(2) if $G_i \equiv \texttt{pause};E_{f(i)}$ and $G_j \equiv \texttt{pause};E_{f(j)}$, $1 \leqslant i,\ j \leqslant n$, $i \neq j$, then $|\vartheta_i| \not\asymp |\vartheta_j|$;

(3) if $G_i \equiv \texttt{pause};E_{f(i)}$ and $G_j \equiv \texttt{exit } T$, $1 \leqslant i,\ j \leqslant n$, then $|\vartheta_i| \not\asymp |\vartheta_j|$;

(4) if either $G_i \equiv \texttt{pause}$ or $G_i \equiv \texttt{nothing}$ then there is no $1 \leqslant j \leqslant n$ such that $\vartheta_i = \vartheta_j \phi$ for some $\phi \in (\mathscr{S}_-^+)^*$, and $G_j \equiv \texttt{pause}$;

(5) if $G_i \equiv \texttt{nothing}$ and $\vartheta_i = \phi_i \gamma$, then there is no $1 \leqslant j \leqslant n$ such that either $\vartheta_j = \phi_i \gamma \psi$ or $\vartheta_j = \phi_i \bar{\gamma} \psi$, for any $\psi \in (\mathscr{S}_-^+)^*$.

(6) if $G_i \equiv \texttt{pause}$ then there is no $1 \leqslant j \leqslant n$ such that $G_j \equiv \texttt{pause};E_{f(j)}$ and $\vartheta_j = \vartheta_i$;

(7) if $G_i \equiv \texttt{pause}$ then, for each ϑ such that $\{s^-, s^+\} \cap |\vartheta| \neq \emptyset$ for every $s \in \mathscr{S}$ and $|\vartheta_i| \subseteq |\vartheta|$, there exists $1 \leqslant j \leqslant n$ such that either $|\vartheta| = |\vartheta_j|$ and $G_j \equiv \texttt{pause};E_{f(j)}$, or $|\vartheta_j| \subseteq |\vartheta|$ and $G_j \equiv \texttt{exit } T$ for some trap T.

Let us consider a normal form $E \equiv F_1 \| \ldots \| F_n$.

Let us assume that $G_i \equiv \texttt{pause}; E_{f(i)}$. Conditions 2 and 3 of Definition 36 imply that if the environment prompts every signal s such that $s^+ \in |\vartheta_i|$ and does not prompt any signal s such that $s^- \in |\vartheta_i|$, so that G_i is executed at this cycle, then $\texttt{nothing} \| \ldots \| \texttt{nothing}; E_{f(i)} \| \ldots \| \texttt{nothing}$ will be executed at the next cycle. In fact, by condition 2, if a statement F_j pauses then $G_j \equiv \texttt{pause}$, $j \neq i$, and, by condition 3, no statement F_j exits any trap, $j \neq i$. Therefore, F_j will behave as `nothing` at the next cycle, for any $j \neq i$.

Condition 4 implies that redundant statements of the form $\texttt{if } \vartheta \texttt{ then pause}$ or of the form $\texttt{if } \vartheta \texttt{ then nothing}$ do not appear as parallel components of E. As an example, the statement E in Example 17 does not satisfy this condition.

Condition 5 implies that redundant statements of the form $\texttt{if } \vartheta \texttt{ then nothing}$ do not appear as parallel components of E. As an example, the statement E in Example 18 does not satisfy this condition.

Condition 6 implies that redundant statements of the form $\texttt{if } \vartheta \texttt{ then pause}$ do not appear as parallel components of E.

Note that conditions 4 and 5 imply that if $F_i \equiv \texttt{if } \vartheta_i \texttt{ then nothing}$ then there exists a label l such that $E \xrightarrow{l}$ and $\vartheta_i n \in \mathscr{E}_l$. Condition 4 implies that if $F_i \equiv \texttt{if } \vartheta_i \texttt{ then pause}$ then there exists a label l such that $E \xrightarrow{l}$ and $\vartheta_i p \in \mathscr{E}_l$.

Axiom seq_1 in Table 6 is justified by the fact that, in both statements, both F and G start exactly when E terminates and, then, they run in parallel.

Note that we do not have the axiom $(E \| F); G = (E; G) \| (F; G)$, since the occurrence of G in $(E \| F); G$ starts when both E and F have terminated, while an occurrence of G in $(E; G) \| (F; G)$ starts when either E or F terminates.

Let us consider axiom seq_2. Given a normal form $E \equiv F_1 \| \ldots \| F_n$, with $F_i \equiv \texttt{if } \vartheta_i \texttt{ then } G_i$, we denote with E^H the statement $F'_1 \| \ldots \| F'_n \| F$, where:

- $$F'_i \equiv \begin{cases} \texttt{if } \vartheta_i \texttt{ then pause}; (E_{f(i)}; H) & \text{if } F_i \equiv \texttt{if } \vartheta_i \texttt{ then pause}; E_{f(i)}, \\ F_i & \text{otherwise;} \end{cases}$$
- $F \equiv \texttt{if } \phi_1 \texttt{ then } H \| \ldots \| \texttt{if } \phi_h \texttt{ then } H$, where $\{\phi_1, \ldots, \phi_h\}$ is the set of ordered events of the form $\psi_{i_1} \ldots \psi_{i_n}$ such that

$$\psi_{i_j} \in \begin{cases} \{\vartheta_{i_j}\} \cup \overline{\vartheta_{i_j}} & \text{if } G_{i_j} \notin \{\texttt{pause}, \texttt{exit } T, \texttt{pause}; E_{f(i_j)}\}, \\ \overline{\vartheta_{i_j}} & \text{otherwise.} \end{cases}$$

Since E is a normal form, if $F_i \equiv \texttt{if } \vartheta_i \texttt{ then pause}; E_{f(i)}$, then we are sure that if the environment prompts every signal s such that $s^+ \in |\vartheta_i|$ and does not prompt any signal s such that $s^- \in |\vartheta_i|$, then E; H pauses and will behave as $E_{f(i)}$; H at the next execution cycle. In this case, the occurrence of H in the body of $\texttt{if } \phi_j \texttt{ then } H$ cannot start at the current cycle, since $|\vartheta_i| \not\gamma |\phi_j|$ for any $1 \leqslant j \leqslant h$ (in fact, ϕ_j contains a string in $\overline{\vartheta_i}$). So, E^H behaves as E; H at the current cycle, and will behave as $E_{f(i)}$; H at the next one.

If E starts and terminates at the current cycle, so that the occurrence of H in the body of E; H starts, then there exists some ϕ_j such that the environment prompts signals as assumed by ϕ_j. Therefore, at least one occurrence of H in the body of E^H starts.

Example 37. As in Examples 21 and 22, let us assume $E \equiv E_1 \parallel E_2$, where
$E_1 \equiv$ `present` s_1 `then exit` T `else nothing end`,
$E_2 \equiv$ `present` s_2 `then emit` s_3 `else nothing end`.
By axiom seq_2, we have E; `emit` $s = E \parallel$ `if` $s_1^- s_2^-$ `then emit` $s \parallel$
`if` $s_1^- s_2^+$ `then emit` $s \parallel$ `if` $s_2^- s_1^-$ `then emit` $s \parallel$ `if` $s_2^+ s_1^-$ `then emit` s.

Axiom seq_3 is straightforward.

Proposition 38. *The axioms in Table* 6 *are sound modulo bisimulation.*

Proof. To prove the soundness of seq_1, let us consider $H \equiv E;(F \parallel G)$ and $H' \equiv (E;F) \parallel (E;G)$, and let us assume that $E \xrightarrow{l_1} E'$, $F \xrightarrow{l_2} F'$ and $G \xrightarrow{l_3} G'$.

If $\mathscr{T}_{l_1} = 1$ then we have $H \xrightarrow{l} E';(F \parallel G)$ iff $H' \xrightarrow{l'} (E';F) \parallel (E';G)$, where $l = l_1 \triangleright (l_2 \otimes l_3)$ and $l' = (l_1 \triangleright l_2) \otimes (l_1 \triangleright l_3)$.

If $\mathscr{T}_{l_1} = 0$, $\mathscr{T}_{l_2}, \mathscr{T}_{l_3} \in \{0,1\}$, then we have $H \xrightarrow{l} F' \parallel G'$ iff $H' \xrightarrow{l'} F' \parallel G'$, where $l = l_1 \triangleright (l_2 \otimes l_3)$ and $l' = (l_1 \triangleright l_2) \otimes (l_1 \triangleright l_3)$.

If either $\mathscr{T}_{l_1} \subseteq \mathscr{T}$ or $\mathscr{T}_{l_1} = 0$ and $\mathscr{T}_{l_2} \subseteq \mathscr{T}$ or $\mathscr{T}_{l_3} \subseteq \mathscr{T}$, then we have $H \xrightarrow{l}$ `nothing` iff $H' \xrightarrow{l'}$ `nothing`, where $l = l_1 \triangleright (l_2 \otimes l_3)$ and $l' = (l_1 \triangleright l_2) \otimes (l_1 \triangleright l_3)$.

Since $l_1 \triangleright (l_2 \otimes l_3) = (l_1 \triangleright l_2) \otimes (l_1 \triangleright l_3)$, it follows that $H \approx H'$.

Let us consider now axiom seq_2. First of all, we note that $\{\phi_1, \ldots, \phi_h\}$ corresponds to the set $I(E)$ used in the definition of function $\triangleright$.

Let us assume that $E \xrightarrow{l_i}$ `nothing` $\parallel \ldots \parallel$ `nothing` with $\mathscr{T}_{l_i} = 0$ and $H \xrightarrow{l'} H'$. We have $E;H \xrightarrow{l} H'$, where

$$l = l_i \triangleright l' = l_i \otimes \left\langle S_{l'}, \bigcup_{\phi \in \mathscr{I}(l_i)} \mathscr{E}^{\phi}_{l'}, \bigcup_{\phi \in \mathscr{I}(E)\setminus\mathscr{I}(l_i)} \mathscr{E}^{\phi}_{l'} \cup \bigcup_{\phi \in \mathscr{I}(E)} \mathscr{N}^{\phi}_{l'}, \mathscr{T}_{l'} \right\rangle.$$

Moreover, we have $E^H \xrightarrow{l''}$ `nothing` $\parallel \ldots \parallel$ `nothing` $\parallel H' \parallel \ldots \parallel H' \parallel$ `nothing` $\parallel \ldots \parallel$ `nothing`, where:

$$l'' = l_i \otimes \bigotimes_{\phi \in \mathscr{I}(l_i)} \langle |\phi| \cup S_{l'}, \mathscr{E}^{\phi}_{l'}, \mathscr{N}^{\phi}_{l'}, \mathscr{T}_{l'} \rangle \otimes \bigotimes_{\phi \in \mathscr{I}(E)\setminus\mathscr{I}(l_i)} \langle S_{\phi}, \emptyset, \mathscr{E}^{\phi}_{l'} \cup \mathscr{N}^{\phi}_{l'}, 0 \rangle.$$

The two derivatives are bisimilar by axioms in Table 2, and $l = l''$ follows by the fact that, for each $\phi \in \mathscr{I}(E)\setminus\mathscr{I}(l_i)$, we have that S_{ϕ} is an event such that $S_{\phi} \subseteq S_{l_i}$, and, for each $\phi \in \mathscr{I}(l_i)$, we have that $|\phi| = S_{l_i} \subseteq S_l$.

Analogously, one can prove that E; $H \xrightarrow{l}$ (`nothing` $\parallel \ldots \parallel$ `nothing`; $E_{f(i)} \parallel \ldots \parallel$ `nothing`); H iff $E^H \xrightarrow{l}$ `nothing` $\parallel \ldots \parallel$ `nothing`;$(E_{f(i)};H) \parallel \ldots \parallel$ `nothing`, where these two derivatives are bisimilar by the fact that `nothing`;$E \approx E$ for every statement E and by axiom $\parallel_3$.

Finally, one can prove that $E;H \xrightarrow{l} \texttt{nothing}$ with $\mathscr{T}_l \subseteq \mathscr{T}$ iff $E^H \xrightarrow{l} \texttt{nothing}$.
It follows that $E;H \approx E^H$.
The soundness of axiom *seq*$_3$ is immediate. □

Let us consider axiom *susp* in Table 7. Given a signal s and a normal form $E \equiv F_1 \| \ldots \| F_n$, we denote with E^s the statement $E^s \equiv F_1^s \| \ldots \| F_n^s$, where

$$F_i^s \equiv \begin{cases} F_i[\texttt{suspend imm } E_{f(i)} \texttt{ when } s/E_{f(i)}] & \text{if } F_i \equiv \texttt{if } \vartheta_i \texttt{ then pause};E_{f(i)}, \\ F_i & \text{otherwise.} \end{cases}$$

Let us consider axiom *trap* in Table 7, a trap name T and a normal form $E \equiv F_1 \| \ldots \| F_n$ such that $F_i \equiv \texttt{if } \vartheta_i \texttt{ then exit } T$, $1 \leqslant i \leqslant m$, and $F_i \equiv \texttt{if } \vartheta_i \texttt{ then } G_i$, $G_i \not\equiv \texttt{exit } T$, $m+1 \leqslant i \leqslant n$. Let us assume that $\vartheta_i = \gamma_{i,1} \ldots \gamma_{i,n_i}$, for $1 \leqslant i \leqslant m$. We denote with $T(E)$ the set of all ordered events $\gamma_{i_1,1} \ldots \overline{\gamma_{i_1,j_{i_1}}} \cdots \gamma_{i_m,1} \cdots \overline{\gamma_{i_m,j_{i_m}}}$, and we assume that $T(E) = \{\phi_1, \ldots, \phi_k\}$. Note that if signals have the status as given by some ϕ_i, $1 \leqslant i \leqslant k$, then no `exit` T is executed. We denote with E^T the statement $E^T \equiv F_1^T \| \ldots \| F_n^T$, where:

$$F_i^T \equiv \begin{cases} F_i[\texttt{trap } T \texttt{ in } E_{f(i)} \texttt{ end}/E_{f(i)}] & \text{if } F_i \equiv \texttt{ if } \vartheta_i \texttt{ then pause};E_{f(i)}, \\ F_i[\texttt{nothing}/\texttt{exit } T] & \text{if } F_i \equiv \texttt{ if } \vartheta_i \texttt{ then exit } T, \\ \texttt{if } \phi_1\vartheta_i \texttt{ then pause} \| \cdots \| & \\ \texttt{if } \phi_k\vartheta_i \texttt{ then pause} & \text{if } F_i \equiv \texttt{if } \vartheta_i \texttt{ then pause}, \\ & |\vartheta_i| \uparrow |\vartheta_j| \text{for some } 1 \leqslant j \leqslant m, \\ F_i & \text{otherwise.} \end{cases}$$

If $F_i \equiv \texttt{if } \vartheta_i \texttt{ then exit } T$, then, since E is a normal form, there exists no j such that $|\vartheta_i| \uparrow |\vartheta_j|$ and $F_j \equiv \texttt{if } \vartheta_j \texttt{ then pause};E_{f(j)}$. Moreover, if $F_j \equiv \texttt{if } \vartheta_j \texttt{ then pause}$ and $|\vartheta_j| \uparrow |\vartheta_h|$ for some $1 \leqslant h \leqslant m$, then we replace F_j by $\texttt{if } \phi_1\vartheta_j \texttt{ then pause} \| \ldots \| \texttt{if } \phi_k\vartheta_j \texttt{ then pause}$. Therefore, the occurrences of `exit` T that are replaced by `nothing` do not preempt any pausing. This justifies axiom *trap*.

Example 39. Let us assume that $\mathscr{S} = \{s_1, s_2\}$ and let us consider statements E and E' such that
$E \equiv \texttt{ if } s_1^+s_2^- \texttt{ then pause};F \parallel \texttt{if } s_1^+ \texttt{ then pause} \parallel \texttt{if } s_2^+ \texttt{ then exit } T$,
$E' \equiv \texttt{ if } s_1^+s_2^- \texttt{ then pause};\texttt{trap } T \texttt{ in } F \texttt{ end} \parallel \texttt{if } s_2^-s_1^+ \texttt{ then pause} \parallel$
$\texttt{if } s_2^+ \texttt{ then nothing}$.
By axiom *trap* we have $\texttt{trap } T \texttt{ in } E \texttt{ end} = E'$.

Proposition 40. *The axioms in Table 7 are sound modulo bisimulation.*

Proof. The soundness of axiom *susp* follows by the following facts:

- $\texttt{suspend } E \texttt{ when } s \xrightarrow{l} \texttt{nothing}$ with $\mathscr{T}_l = 0$ iff $E^s \xrightarrow{l} \texttt{nothing} \| \ldots \| \texttt{nothing}$, where $\texttt{nothing} \approx \texttt{nothing} \| \ldots \| \texttt{nothing}$ by axiom $\|_3$;
- $\texttt{suspend } E \texttt{ when } s \xrightarrow{l} \texttt{nothing}$ with $\mathscr{T}_l \subseteq \mathscr{T}$ iff $E^s \xrightarrow{l} \texttt{nothing}$;
- $\texttt{suspend } E \texttt{ when } s \xrightarrow{l} \texttt{suspend imm}(\texttt{nothing} \| \ldots \| \texttt{nothing}; E_{f(i)} \| \ldots \| \texttt{nothing})$ `when` s if and only if

$E^s \xrightarrow{l}$ `nothing` $\| \ldots \|$ `nothing`; `suspend imm` $E_{f(i)}$ `when` $s \| \ldots \|$ `nothing`, where these two derivatives are bisimilar by axiom $\|_3$ and by the fact that `nothing`; $E \approx E$ for any statement E.

Let us consider now axiom *trap*. We have `trap` T `in` E `end` $\xrightarrow{l}$ `nothing` with $\mathscr{T}_l = 0$ if and only if either $E \xrightarrow{l'}$ `nothing` $\| \ldots \|$ `nothing` with $\mathscr{T}_{l'} = 0$, or $E \xrightarrow{l'}$ `nothing` with $\mathscr{T}_{l'} = \{T\}$. In both cases, $l = tr(T, l')$.

Now, $E \xrightarrow{l'}$`nothing` $\| \ldots \|$ `nothing` iff $E^T \xrightarrow{l''}$`nothing` $\| \ldots \|$ `nothing`, and $E \xrightarrow{l'}$ `nothing` with $\mathscr{T}_{l'} = \{T\}$ iff $E^T \xrightarrow{l''}$`nothing` $\| \ldots \|$ `nothing`.

In both cases, we have $l'' = l$ by the definition of $tr(T, l')$, and `nothing` $\approx$ `nothing` $\| \ldots \|$ `nothing` by axiom $\|_3$.

We have

`trap` T `in` E `end` $\xrightarrow{l}$ `trap` T`in nothing` $\| \ldots \|$ `nothing`; $E_{f(i)}$ $\| \ldots \|$ `nothing end`

if and only if

$E \xrightarrow{l'}$ `nothing` $\| \ldots \|$ `nothing`; $E_{f(i)}$ $\| \ldots \|$ `nothing`

if and only if

$E^T \xrightarrow{l''}$`nothing` $\| \ldots \|$ `nothing`; `trap` T `in` $E_{f(i)}$ `end` $\| \ldots \|$ `nothing`,

where $l'' = l$ by the definition of $tr(T, l')$, and `trap` T `in nothing` $\| \ldots \|$ `nothing`; $E_{f(i)}$ $\| \ldots \|$ `nothing end` $\approx$ `nothing` $\| \ldots \|$ `nothing`; `trap` T `in` $E_{f(i)}$ `end` $\| \ldots \|$ `nothing` by axiom $\|_3$ and by the fact that `nothing`; $E \approx E$ for any statement E.

Finally, we have `trap` T `in` $E \xrightarrow{l}$`nothing` with $\mathscr{T}_l \subseteq \mathscr{T}$, $\mathscr{T}_l \neq \{T\}$, if and only if $E \xrightarrow{l'}$ `nothing` with $\mathscr{T}_{l'} \subseteq \mathscr{T}$, $\mathscr{T}_{l'} \neq \{T\}$, if and only if $E^T \xrightarrow{l''}$`nothing` with $\mathscr{T}_{l''} \subseteq \mathscr{T}$, $\mathscr{T}_{l''} \neq \{T\}$, and $l'' = l$ by the definition of $tr(T, l')$. □

Let us consider axiom s_1 in Table 8. This is justified by the fact that s is not in the input–output interface of statement `signal` s `in` E `end`.

Let us consider axiom s_2. Given a normal form $E \equiv F_1 \| \ldots \| F_n$ and a signal s, we denote with E_s the statement $E_s \equiv F_{s,1} \| \ldots \| F_{s,n}$, where

$$F_{s,i} \equiv \begin{cases} F_i\ [\texttt{signal}\ s\ \texttt{in}\ E_{f(i)}\ \texttt{end}/E_{f(i)}] & \text{if } F_i \equiv \texttt{if}\ \vartheta_i\ \texttt{then pause}; E_{f(i)}, \\ F_i & \text{otherwise.} \end{cases}$$

Axiom s_2 is justified by two facts. The first is that the status of signals does not propagate between two execution cycles. The second is that, since E is a normal form, if it pauses then it will behave as `nothing` $\| \ldots \|$ `nothing`; $E_{f(i)}$ $\| \ldots \|$ `nothing` at the next execution cycle, for some $1 \leqslant i \leqslant n$. So, it does not matter whether s is local to $E_{f(i)}$ or to `nothing` $\| \ldots \|$ `nothing`; $E_{f(i)}$ $\| \ldots \|$ `nothing`.

Note that it is essential that E is a normal form. In fact, as an example, we do not have, in general, $H \approx K$, for H and K statements such that

$H \equiv$ `signal` s `in (pause;` E `‖ pause;` F`) end`,

$K \equiv$ `signal` s `in (pause; signal` s `in` E `end ‖ pause; signal` s `in` F `end) end`.

In fact, at the second execution cycle, statements E and F in the body of H view the same signal s, and this cannot happen for E and F in the body of K.

Let us consider axiom s_3 and a constructive normal form $E \equiv F_1 \| \ldots \| F_n$.

Let us denote with Θ_{s^+} and Θ_{s^-} the following sets of ordered events:

$\Theta_{s^+} = \{\vartheta_i \mid 1 \leqslant i \leqslant n, s^-, s^+ \notin |\vartheta_i|, G_i \equiv \texttt{emit } s\}$; $\Theta_{s^-} = \{\phi_{i_1} \ldots \phi_{i_m} \mid$ for each $1 \leqslant j \leqslant m$ we have $G_{i_j} \equiv \texttt{emit } s, \phi_{i_j} \in \overline{\vartheta_{i_j}}$, $\phi_{i_j} = \phi'_{i_j}\gamma_{i_j}$ and $\gamma_{i_j} \notin \{s^+, s^-\}\}$.

Note that if the environment prompts every signal s with $s^+ \in |\vartheta|$ and does not prompt any signal s with $s^- \in |\vartheta|$, for some $\vartheta \in \Theta_{s^+}$, then E emits s. On the contrary, if the environment prompts every signal s with $s^+ \in |\vartheta|$ and does not prompt any signal s with $s^- \in |\vartheta|$, for some $\vartheta \in \Theta_{s^-}$, then E does not emit s.

Let $G_{s,i}$ be the statement such that $F_{s,i} \equiv \texttt{if } \vartheta_i \texttt{ then } G_{s,i}$.

Let us denote with $G_i \backslash \{s\}$ the statement

$$G_i \backslash \{s\} \equiv \begin{cases} \texttt{nothing} & \text{if } G_{s,i} \equiv \texttt{emit } s, \\ G_{s,i} & \text{otherwise.} \end{cases}$$

Let us denote with $F_i \backslash \{s\}$ the following statement:

$$F_i \backslash \{s\} \equiv \|_{(\vartheta \in \Theta_{s^+}, \phi \in \Theta_{s^-})} \texttt{ if } \vartheta_i[\vartheta/s^+][\phi/s^-] \texttt{ then } G_i \backslash \{s\}.$$

Finally, let us denote with $E \backslash \{s\}$ the statement $E \equiv F_1 \backslash \{s\} \| \ldots \| F_n \backslash \{s\}$. Intuitively, axiom s_3 replaces occurrences of `emit` s by `nothing`, replaces every test for the presence of s by a set of tests, each for the presence of an event causing s, and replaces every test for the absence of s by a set of tests, each for the absence of all events causing s.

Example 41. Let a, b, c, d and s signals in $\mathscr{S}$. Let E and E' be the statements $E \equiv$ `if` a^+ `then emit` $s \parallel$ `if` b^+ `then emit` $s \parallel$ `if` s^+ `then emit` $c \parallel$ `if` s^- `then emit` d,

$E' \equiv$ `if` a^+ `then nothing` $\parallel$ `if` b^+ `then nothing` $\parallel$ `if` a^+ `then emit` $c \parallel$ `if` b^+ `then emit` $c \parallel$ `if` $a^- b^-$ `then emit` $d \parallel$ `if` $b^- - a^-$ `then emit` $d \parallel$.

By axioms s_3 we have `signal` s `in` E `end` $= E'$.

Proposition 42. *The axioms in Table* 8 *are sound modulo bisimulation.*

Proof. The soundness of axiom s_1 follows by the fact that $loc(s, loc(s, l))$ is defined if and only if $loc(s, l)$ is. Moreover, if $loc(s, l)$ is defined, then $loc(s, loc(s, l)) = loc(s, l)$.

The soundness of axiom s_2 follows by the following facts:

- `signal` s `in` E `end` $\xrightarrow{l}$ `signal` s `in` (`nothing` $\| \ldots \|$ `nothing`; $E_{f(i)} \| \ldots \|$ `nothing`) `end` with $\mathscr{T}_l = 1$ if and only if `signal` s `in` E_s `end` $\xrightarrow{l}$ `signal` s `in` (`nothing` $\| \ldots \|$ `nothing`; `signal` s `in` $E_{f(i)}$ `end` $\| \ldots \|$ `nothing`) `end`, and the two derivatives are bisimilar by axioms s_1 and $\|_3$.
- `signal` s `in` E `end` $\xrightarrow{l}$ `signal` s `in` (`nothing` $\| \ldots \|$ `nothing`) `end` with $\mathscr{T}_l = 0$ iff `signal` s `in` E_s `end` $\xrightarrow{l}$ `signal` s `in` (`nothing` $\| \ldots \|$ `nothing`) `end`.
- `signal` s `in` E `end` $\xrightarrow{l}$ `signal` s `in nothing end` with $\mathscr{T}_l \subseteq \mathscr{T}$ iff `signal` s `in` E_s `end` $\xrightarrow{l}$ `signal` s `in nothing end`.

Let us consider now axiom s_3. We must prove that $\texttt{signal}\ s\ \texttt{in}\ E_s\ \texttt{end} \xrightarrow{l} H$ iff $E\backslash\{s\} \xrightarrow{l'} H'$, where $l = l'$ and $H \approx H'$.

Now, $\texttt{signal}\ s\ \texttt{in}\ E_s\ \texttt{end} \xrightarrow{l} H$ iff $F_{s,i} \xrightarrow{l_i} H_i$, $l = loc(s, l_1 \otimes \cdots \otimes l_n)$, and $H \equiv \texttt{signal}\ s\ \texttt{in}\ H_1 \| \cdots \| H_n\ \texttt{end}$.

Analogously, $E\backslash\{s\} \xrightarrow{l'} H'$ iff $F_i\backslash\{s\} \xrightarrow{l'_i} H'_i$, $l' = l'_1 \otimes \cdots \otimes l'_n$, and $H' \equiv H'_1 \| \ldots \| H'_n$.

Axioms $\|_1$ and $\|_2$ imply that we can assume $G_1, \ldots, G_v \equiv \texttt{emit}\ s$ and $G_{v+1}, \ldots, G_n \not\equiv \texttt{emit}\ s$, for some $0 \leqslant v \leqslant n$.

We distinguish between the case with $s \in Em(l_1 \otimes \cdots \otimes l_n)$ and the case with $s \notin Em(l_1 \otimes \cdots \otimes l_n)$.

- $s \in Em(l_1 \otimes \cdots \otimes l_n)$.

  For every $1 \leqslant i \leqslant v$, we have $F_{s,i} \xrightarrow{l_i} \texttt{nothing}$ with either $\mathscr{E}_{l_i} = \{\vartheta_i s\}$ or $\mathscr{N}_{l_i} = \{\vartheta_i s\}$. By axioms $\|_1$ and $\|_2$ we can assume that $\vartheta_i s \in \mathscr{E}_{l_i}$ for $1 \leqslant i \leqslant u$, and $\vartheta_i s \in \mathscr{N}_{l_i}$ for $u+1 \leqslant i \leqslant v$.

  We deduce $l = l'$ and $H \approx H'$ by the following facts:

  ∘ For an arbitrary $1 \leqslant j \leqslant n$, $F_{s,j} \xrightarrow{l_j} H_j$ with $\mathscr{E}_{l_j} = \{\vartheta s^+ \psi\mu\}$ iff $F_j\backslash\{s\} \xrightarrow{l'_j} H_j \| \ldots \| H_j \| \texttt{nothing} \| \ldots \| \texttt{nothing}$, where $\mathscr{E}_{l'_j} = \{\vartheta\vartheta_i\psi\mu[n/s] \mid \vartheta_i \in \Theta_{s^+}, 1 \leqslant i \leqslant u\}$, $\mathscr{N}_{l'_j} = \{\vartheta\vartheta_i\psi\mu[n/s] \mid \vartheta_i \in \Theta_{s^+}, u+1 \leqslant i \leqslant v\}$.
  So, $\vartheta\vartheta_i\psi\mu[n/s] \in \mathscr{E}_l$ iff $\vartheta\vartheta_i\psi\mu[n/s] \in \mathscr{E}_{l'}$, $1 \leqslant i \leqslant u$, $\vartheta\vartheta_i\psi\mu[n/s] \in \mathscr{N}_l$ iff $\vartheta\vartheta_i\psi\mu[n/s] \in \mathscr{N}_{l'}$, $u+1 \leqslant i \leqslant v$.

  ∘ For an arbitrary $1 \leqslant j \leqslant n$, $F_{s,j} \xrightarrow{l_j} \texttt{nothing}$ with $\mathscr{N}_{l_j} = \{\vartheta s^+ \psi\mu\}$ iff $F_j\backslash\{s\} \xrightarrow{l'_j} \texttt{nothing} \| \ldots \| \texttt{nothing}$, $\mathscr{N}_{l'_j} = \{\vartheta\vartheta_i\psi\mu[n/s] \mid \vartheta_i \in \Theta_{s^+}\}$. So, $\vartheta\vartheta_i\psi\mu[n/s] \in \mathscr{N}_l$ iff $\vartheta\vartheta_i\psi\mu[n/s] \in \mathscr{N}_{l'}$, $1 \leqslant i \leqslant v$.

  ∘ For an arbitrary $1 \leqslant j \leqslant n$, $F_{s,j} \xrightarrow{l_j} \texttt{nothing}$ with $\mathscr{N}_{l_j} = \{\vartheta s^- \psi\mu\}$ iff $F_j\backslash\{s\} \xrightarrow{l'_j} \texttt{nothing} \| \ldots \| \texttt{nothing}$, $\mathscr{N}_{l'_j} = \{\vartheta\phi\psi\mu[n/s] \mid \phi \in \Theta_{s^-}\}$. So, $\vartheta\phi\psi\mu[n/s] \in \mathscr{N}_l$ iff $\vartheta\phi\psi\mu[n/s] \in \mathscr{N}_{l'}$, $\phi \in \Theta_{s^-}$.

  ∘ For an arbitrary $1 \leqslant j \leqslant n$, $F_{s,j} \xrightarrow{l_j} H_j$, $\vartheta\mu \in \mathscr{E}_{l_j}$ (resp. $\vartheta\mu \in \mathscr{N}_{l_j}$), $\{s^-, s^+\} \cap |\vartheta| = \emptyset$, $\mu \neq s$, iff $F_j\backslash\{s\} \xrightarrow{l'_j} H_j$, $\vartheta\mu \in \mathscr{E}_{l'_j}$ (resp. $\vartheta\mu \in \mathscr{N}_{l'_j}$).

- $s \notin Em(l_1 \otimes \cdots \otimes l_n)$.

  For every $1 \leqslant i \leqslant v$ we have $F_{s,i} \xrightarrow{l_i} \texttt{nothing}$ with $\mathscr{N}_{l_i} = \{\vartheta_i s\}$.
  We deduce $l = l'$ and $H \approx H'$ by the following facts:

  ∘ For an arbitrary $1 \leqslant j \leqslant n$, $F_{s,j} \xrightarrow{l_j} H_j$ with $\mathscr{E}_{l_j} = \{\vartheta s^- \psi\mu\}$ iff $F_j\backslash\{s\} \xrightarrow{l'_j} H_j \| \ldots \| H_j \| \texttt{nothing} \| \ldots \| \texttt{nothing}$ with $\mathscr{E}_{l'_j} = \{\vartheta\phi\psi\mu \mid \phi \in \Theta_{s^-}, |\phi| \notin S_{l_1} \cup \cdots \cup S_{l_v}\}$, $\mathscr{N}_{l'_j} = \{\vartheta\phi\psi\mu \mid \phi \in \Theta_{s^-}, |\phi| \notin S_{l_1} \cup \cdots \cup S_{l_v}\}$.

    So, we have that $\vartheta\phi\psi\mu \in \mathscr{E}_l$ iff $\vartheta\phi\psi\mu \in \mathscr{E}_{l'}$, and $\vartheta\phi\psi\mu \in \mathscr{N}_l$ iff $\vartheta\phi\psi\mu \in \mathscr{N}_{l'}$, $\phi \in \Theta_{s^-}$.

  ∘ For an arbitrary $1 \leqslant j \leqslant n$, $F_{s,j} \xrightarrow{l_j} \texttt{nothing}$ with $\mathscr{N}_{l_j} = \{\vartheta s^- \psi\mu\}$ iff $F_j\backslash\{s\} \xrightarrow{l'_j} \texttt{nothing} \| \ldots \| \texttt{nothing}$, $\mathscr{N}_{l'_j} =, \{\vartheta\phi\psi\mu[n/s] \mid \phi \in \Theta_{s^-}\}$. So, $\vartheta\phi\psi\mu[n/s] \in \mathscr{N}_l$ iff $\vartheta\phi\psi\mu[n/s] \in \mathscr{N}_{l'}$, $\phi \in \Theta_{s^-}$.

  ∘ For an arbitrary $1 \leqslant j \leqslant n$, $F_{s,j} \xrightarrow{l_j} \texttt{nothing}$ with $\mathscr{N}_{l_j} = \{\vartheta s^+ \psi\mu\}$ iff $F_j\backslash\{s\} \xrightarrow{l'_j}$

`nothing` $\| \ldots \|$ `nothing`, $\mathscr{N}_{l'_j} = \{\vartheta\vartheta_i\psi\mu[n/s] \mid \vartheta_i \in \Theta_{s^+}\}$. So, $\vartheta\vartheta_i\psi\mu[n/s] \in \mathscr{N}_l$ iff $\vartheta\vartheta_i\psi\mu[n/s] \in \mathscr{N}_{l'}$, $1 \leqslant i \leqslant v$.

∘ For an arbitrary $1 \leqslant j \leqslant n$, $F_{s,j} \xrightarrow{l_j} H_j$, $\vartheta\mu \in \mathscr{E}_{l_j}$ (resp. $\vartheta\mu \in \mathscr{N}_{l_j}$), $\{s^-, s^+\} \cap |\vartheta| = \emptyset$, $\mu \neq s$, iff $F_j \backslash \{s\} \xrightarrow{l'_j} H_j$, $\vartheta\mu \in \mathscr{E}_{l'_j}$ (resp. $\vartheta\mu \in \mathscr{N}_{l'_j}$). □

We can prove now the soundness of our axiomatization.

Lemma 43. *Given Esterel statements E and E', $E = E'$ implies $E \approx E'$.*

Proof. Up to now we have proved the soundness modulo bisimulation over Esterel$^+$ of the axioms in Tables 2–8. Since the TSS for Esterel$^+$ is an operational conservative extension of the TSS for Esterel (see Proposition 31), we infer that the axiomatization is sound modulo bisimulation over Esterel. □

4.2. The proof of completeness

We must prove now that the axioms in Tables 2–8 give an axiomatization complete modulo bisimulation on constructive Esterel statements.

We follow the proof technique proposed in [24]. First of all we prove that, given an arbitrary constructive Esterel statement E, there exists a normal form E' such that $E = E'$ and all derivatives of E' are normal forms (Lemma 44). Then, we introduce the notion of guarded recursive specification and we prove that every guarded recursive specification has a solution which is unique modulo $=$ (Lemma 45). Finally, we exploit these two results to prove that two arbitrary constructive Esterel statements E and E' such that $E \approx E'$ are equated by axioms in Tables 2–8 (Lemma 46). In fact, we prove that $E = F$ and $E' = F'$, where F and F' are normal forms and solutions of the same guarded recursive specification.

We begin with introducing some notations.

We say that a variable P is *strongly guarded* in an Esterel$^+$ statement E if P is guarded in E, and no free occurrence of P appears in the left side of a ";" or in the body of statements `suspend`, `signal`, `trap` and `loop`.

An Esterel$^+$ statement E is *well formed* if and only if:

- for each statement `rec` $P.F$ in the body of E, the variable P is strongly guarded in F;
- every variable $P \in Free(E)$ is strongly guarded in E.

Note that our axioms transform well-formed statements into well-formed statements. Note also that every Esterel statement E is well formed, since no variable appears in E.

The following lemma states that an arbitrary constructive Esterel statement E can be transformed, by applying axioms, into a normal form that has only normal forms as derivatives.

Lemma 44. *Given a well-formed constructive Esterel$^+$ statement E, there exist normal forms $E_1,\ldots,E_m$ such that*:

- $E_i = F_{i,1} \| \ldots \| F_{i,n_i}$, $F_{i,j} \equiv \texttt{if } \vartheta_{i,j} \texttt{ then } G_{i,j}$, *and, if* $G_{i,j} \equiv \texttt{pause}; E_{f(i,j)}$, *then* $f_{(i,j)} \in \{1,\ldots,m\}$;
- $E = E_1$.

Proof. By structural induction on E.

Base case: If E is a basic statement, $E \not\equiv \texttt{pause}$, then the thesis is immediate, since E is a normal form. If $E \equiv \texttt{pause}$, then, by axiom seq_3 we infer $E = \texttt{pause; nothing}$, and, by axioms $\|_5$ and $\|_6$, we infer $\texttt{pause; nothing} = \texttt{pause} \parallel \texttt{if } s_1^+ \ldots s_{|\mathscr{S}|}^+ \texttt{ then pause; nothing} \parallel \ldots \parallel \texttt{if } s_1^- \ldots s_{|\mathscr{S}|}^- \texttt{ then pause; nothing}$, which is a normal form.

Induction step: As inductive hypothesis, let us assume that, given statements E' and E'', there exist normal forms $E_{1'},\ldots,E_{m'}$, $E_{1''},\ldots,E_{m''}$, such that $E_{i'} = F_{i',1} \| \ldots \| F_{i',n_{i'}}$, $E_{i''} = F_{i'',1} \| \ldots \| F_{i'',n_{i''}}$, $F_{i',j} \equiv \texttt{if } \vartheta_{i',j} \texttt{ then } G_{i',j}$, $F_{i'',j} \equiv \texttt{if } \vartheta_{i'',j} \texttt{ then } G_{i'',j}$, $E' = E_{1'}$, $E'' = E_{1''}$.

We consider the following cases:

- $E \equiv E' \parallel E''$.
  Since $E' = E_{1'}$, $E'' = E_{1''}$ and $=$ is a congruence, we infer $E = E_{1'} \parallel E_{1''}$. Let us denote with $\mathscr{I} \subseteq \{1',\ldots,m'\} \times \{1'',\ldots,m''\}$ the least set such that:
  - $(1',1'') \in \mathscr{I}$;
- as a parallel composition of normal forms having only normal
  - if $(i',i'') \in \mathscr{I}$, $F_{i',j'} \equiv \texttt{if } \vartheta_{i',j'} \texttt{ then pause; } E_{f(i',j')}$, $F_{i'',j''} \equiv \texttt{if } \vartheta_{i'',j''} \texttt{ then pause; } E_{f(i'',j'')}$ and $|\vartheta_{i',j'}| \uparrow |\vartheta_{i'',j''}|$ then $(f(i',j'), f(i'',j'')) \in \mathscr{I}$.

  The thesis follows if we infer $E_{i'} \,||\, E_{i''} = E_{i',i''}$, with $E_{i',i''}$ an arbitrary normal form having only normal forms as derivatives, for every $(i',i'') \in \mathscr{I}$.

  Statement $E_{i'} \,||\, E_{i''}$ satisfies Condition 1 of Definition 36, provided that we remove every component $F_{i'',j''}$ such that $F_{i'',j''} \equiv F_{i',j'}$, for some $1 \leqslant j' \leqslant n_{i'}$, by means of axioms $||_1$, $||_2$ and $||_4$.

  By applying axiom $||_7$, we infer $E_{i'} \,||\, E_{i''} = F_{i',i''}$, for a statement $F_{i',i''}$ satisfying Conditions 1 and 2 of Definition 36.

  By applying axiom $||_8$, we infer $F_{i',i''} = G_{i',i''}$, for a statement $G_{i',i''}$ satisfying Conditions 1–3 of Definition 36.

  By applying axioms $||_6$ and $||_9$, we infer $G_{i',i''} = H_{i',i''}$, for a statement $H_{i',i''}$ satisfying Conditions 1–4 of Definition 36.

  By applying axioms $?_2$, $?_3$ and $||_3$, we infer $H_{i',i''} = K_{i',i''}$, for a statement $K_{i',i''}$ satisfying Conditions 1–5 of Definition 36. In fact, let us assume that $H_{i',i''}$ does not satisfy Condition 5 of Definition 36, namely $H_{i',i''} \equiv H_1 \,||\, \ldots \,||\, H_n$, where there exist $1 \leqslant h,\ k \leqslant n$ such that $H_h \equiv \texttt{if } \vartheta_h \texttt{ then nothing}$, $H_k \equiv \texttt{if } \vartheta_k \texttt{ then } G_k$, $\vartheta_h = \phi_h\gamma$, and either $\vartheta_k = \phi_h\gamma\psi$, or $\vartheta_k = \phi_h\bar{\gamma}\psi$, for some $\psi \in (\mathscr{S}_-^+)^*$. Since $\texttt{if } \phi_h\gamma \texttt{ then nothing}$ and $\texttt{if } \phi_h\bar{\gamma} \texttt{ then nothing}$ denote the same statement, we can assume

the first case. By axioms $||_1$ and $||_2$ we can assume $h=1$ and $k=2$. Now, we infer
$\texttt{if } \vartheta_1 \texttt{ then nothing } || \texttt{ if } \vartheta_1 \texttt{ then (if } \psi \texttt{ then } G_2) =$
$\texttt{if } \vartheta_1 \texttt{ then (nothing } || \texttt{ if } \psi \texttt{ then } G_2) =$
$\texttt{if } \vartheta_1 \texttt{ then (if } \psi \texttt{ then } G_2) \equiv H_2,$
where the equalities are inferred by means of axioms $?_2$ and $?_3$ and by means of axiom $||_3$, respectively.

Finally, by axioms seq_1, seq_3, $?_2$, $?_3$ and $||_3$ we infer $K_{i',i''} = I_{i',i''}$ for a statement $I_{i',i''}$ satisfying Conditions 1–6 of Definition 36. In fact, let us assume that $K_{i',i''}$ does not satisfy Condition 6 of Definition 36, namely $K_{i',i''} \equiv K_1 || \ldots || K_n$, where $K_i \equiv \texttt{if } \vartheta \texttt{ then pause}$, $K_j \equiv \texttt{if } \vartheta \texttt{ then pause}; K$. By axioms $||_1$ and $||_2$ we can assume $i=1$ and $j=2$. Now, we have
$\texttt{if } \vartheta \texttt{ then pause}; K =$
$\texttt{if } \vartheta \texttt{ then pause}; (K \texttt{ || nothing}) =$
$\texttt{if } \vartheta \texttt{ then ((pause}; K) \texttt{ || (pause; nothing))} =$
$\texttt{if } \vartheta \texttt{ then (pause}; K) \texttt{ || if } \vartheta \texttt{ then (pause; nothing)} =$
$\texttt{if } \vartheta \texttt{ then (pause}; K) \texttt{ || if } \vartheta \texttt{ then pause},$
where the equalities are obtained by means of axiom $||_3$, axiom seq_1, axioms $?_2$ and $?_3$, and axiom seq_3, respectively.

Note that $I_{i',i''}$ satisfies also Condition 7 of Definition 36, since $E_{i'}$ and $E_{i''}$ do. So, we can take $E_{i',i''} \equiv I_{i',i''}$.

- $E \equiv \texttt{present } s \texttt{ then } E' \texttt{ else } E'' \texttt{ end}.$
  Since $E' = E_{1'}$, $E'' = E_{1''}$ and $=$ is a congruence, we infer
  $E = \texttt{present } s \texttt{ then } E_{1'} \texttt{ else } E_{1''} \texttt{ end}.$
  By axiom $?_1$ we infer
  $\texttt{present } s \texttt{ then } E_{1'} \texttt{ else } E_{1''} \texttt{ end} = \texttt{if } s^+ \texttt{ then } E_{1'} \texttt{ || if } s^- \texttt{ then } E_{1''}.$
  By axioms $?_2$ and $?_3$ we infer
  $\texttt{if } s^+ \texttt{ then } E_{1'} \texttt{ || if } s^- \texttt{ then } E_{1''} =$
  $\texttt{if } s^+ \texttt{ then } F_{1',1} || \ldots || \texttt{ if } s^+ \texttt{ then } F_{1',n_{1'}} \texttt{ || if } s^- \texttt{ then } F_{1'',1} || \ldots || \texttt{ if } s^- \texttt{ then } F_{1'',n_{1''}},$
  which satisfies all conditions of Definition 36.
- $E = E'; E''.$
  Since $E' = E_{1'}$, $E'' = E_{1''}$ and $=$ is a congruence, we infer $E = E_{1'}; E_{1''}$. Then we infer $E_{1'}; E_{1''} = E_{1'}^{E_{1''}}$ by axiom seq_2, and the thesis follows as in the case of $||$.
- $E \equiv \texttt{rec } P.E'.$
  Let us consider statements $H_{1'}, \ldots, H_{m'}$ s.t. $H_{i'} \equiv E_{i'}[E/P]$, $1 \leqslant i' \leqslant m'$.
  We have $H_{i'} \equiv E_{i'}[E/P] \equiv (F_{i',1} || \ldots || F_{i',n_{i'}})[E/P] \equiv$
  $F_{i',1}[E/P] || \ldots || F_{i',n_{i'}}[E/P] \equiv$
  $F_{i',1}[H_{f(i',1)}/E_{f(i',1)}][E/P] || \ldots || F_{i',n_{i'}}[H_{f(i',n_{i'})}/E_{f(i',n_{i'})}][E/P] =$
  $F_{i',1}[H_{f(i',1)}/E_{f(i',1)}][E'[E/P]/P] \; || \ldots$
  $\ldots || F_{i',n_{i'}}[H_{f(i',n_{i'})}/E_{f(i',n_{i'})}][E'[E/P]/P] =$
  $F_{i',1}[H_{f(i',1)}/E_{f(i',1)}][E_{1'}[E/P]/P] || \ldots$
  $\ldots || F_{i',n_{i'}}[H_{f(i',n_{i'})}/E_{f(i',n_{i'})}][E_{1'}[E/P]/P] \equiv$
  $F_{i',1}[H_{f(i',1)}/E_{f(i',1)}][H_{1'}/P] || \ldots || F_{i',n_{i'}}[H_{f(i',n_{i'})}/E_{f(i',n_{i'})}][H_{1'}/P],$

where the equalities are inferred by axiom rec_1 and by the fact that $=$ is a congruence. Now, $H_{i'}$ has been rewritten as a parallel composition of normal forms having only normal forms as derivatives, where no free occurrence of P appears. Let us call $K_{i'}$ such statement. Every $K_{i'}$ can be transformed into a normal form as in the case for "||". Finally, the thesis follows since we have $E = E'[E/P] = E_{1'}[E/P] \equiv H_{1'}$.

- $E \equiv \texttt{loop}\ E'\ \texttt{end}$.
  By axiom $loop_1$ we infer $E = \texttt{rec}\, P.(E'; P)$, so that the thesis follows as in the case for construct `rec`.
- $E \equiv \texttt{signal}\ s\ \texttt{in}\ E'\ \texttt{end}$.
  Since $E' = E_{1'}$ and $=$ is a congruence, we infer $E = \texttt{signal}\ s\ \texttt{in}\ E_{1'}\ \texttt{end}$.
  Let us consider an arbitrary $1 \leqslant i' \leqslant m'$. By axiom s_2 we have
  $\texttt{signal}\ s\ \texttt{in}\ E_{i'}\ \texttt{end} = \texttt{signal}\ s\ \texttt{in}\ E_{i's}\ \texttt{end}$, where $E_{i's}$ is a normal form.
  By axiom s_3 we have: $\texttt{signal}\ s\ \texttt{in}\ E_{i's}\ \texttt{end} = E_{i'} \backslash \{s\}$. (We can apply axiom s_3 since E is constructive by the hypothesis and our axioms preserve constructiveness.)
  Now, $E_{i'} \backslash \{s\} \equiv K_{i',1,1} || \ldots || K_{i',1,t_{i',1}} || \ldots || K_{i',n_{i'},1} || \ldots || K_{i',n_{i'},t_{i',n_{i'}}}$, where:
  - $K_{i',j,h} \equiv \texttt{if}\ \vartheta_{i',j,h}\ \texttt{then pause; signal}\ s\ \texttt{in}\ E_{f(i',j)}\ \texttt{end}$,
    if $F_{i',j} \equiv \texttt{if}\ \vartheta_{i',j}\ \texttt{then pause}; E_{f(i',j)}$;
  - $K_{i',j,h} \equiv \texttt{if}\ \vartheta_{i',j,h}\ \texttt{then nothing}$, if $F_{i',j} \equiv \texttt{if}\ \vartheta_{i',j}\ \texttt{then emit}\ s$;
  - $K_{i',j,h} \equiv \texttt{if}\ \vartheta_{i',j,h}\ \texttt{then}\ G_{i',j}$, otherwise.
    Namely:
  - $K_{i',j,h} = \texttt{if}\ \vartheta_{i',j,h}\ \texttt{then pause}; E_{f(i',j)} \backslash \{s\}$,
    if $F_{i',j} \equiv \texttt{if}\ \vartheta_{i',j}\ \texttt{then pause}; E_{f(i',j)}$;
  - $K_{i',j,h} = \texttt{if}\ \vartheta_{i',j,h}\ \texttt{then nothing}$, if $F_{i',j} \equiv \texttt{if}\ \vartheta_{i',j}\ \texttt{then emit}\ s$;
  - $K_{i',j,h} = \texttt{if}\ \vartheta_{i',j,h}\ \texttt{then}\ G_{i',j}$, otherwise.
    So, $E_{i'} \backslash \{s\}$ has been rewritten as a parallel composition of normal forms having only normal forms as derivatives. Let us call $K_{i'}$ such a statement. Every $K_{i'}$ can be transformed into a normal form $H_{i'}$ as in the case of "||". So, $H_{1'}, \ldots H_{m'}$ are the statements we were looking for, and $E = H_{1'}$.
- $E \equiv \texttt{trap}\ T\ \texttt{in}\ E'\ \texttt{end}$.
  Since $E' = E_{1'}$ and $=$ is a congruence, we infer $E = \texttt{trap}\ T\ \texttt{in}\ E_{1'}\ \texttt{end}$.
  By axiom *trap*, we have $\texttt{trap}\ T\ \texttt{in}\ E_{i'}\ \texttt{end} = E^T_{i'}$, and $E^T_{i'} \equiv F^T_{i',1} || \ldots || F^T_{i',n_{i'}}$, where
  $F^T_{i',j} =$

$$\begin{cases} F_{i',j}[E^T_{f(i',j)}/E_{f(i',j)}] & \text{if } F_{i',j} \equiv\ \texttt{if}\ \vartheta_{i',j}\ \texttt{then pause}; E_{f(i',j)}, \\ F_{i',j}\ [\texttt{nothing/exit}\ T] & \text{if } F_{i',j} \equiv \texttt{if}\ \vartheta_{i',j}\ \texttt{then exit}\ T, \\ \texttt{if}\ \phi_1\vartheta_{i',j}\ \texttt{then pause} || \ldots & \\ \ldots || \ \texttt{if}\ \phi_k\vartheta_{i',j}\ \texttt{then pause} & \text{if } F_{i',j} \equiv \texttt{if}\ \vartheta_{i',j}\ \texttt{then pause} \\ & |\vartheta_{i',j}| \uparrow |\vartheta_{i',h}|, G_{i',h} \equiv \texttt{exit}\ T, \\ F_{i',j} & \text{otherwise.} \end{cases}$$

Now, $E_{i'}^T$ has been rewritten as a parallel composition of normal forms, having only normal forms as derivatives. Let us call $K_{i'}$ such a statement. Every $K_{i'}$ can be transformed into a normal form $H_{i'}$ as in the case of "||". So, $H_{1'},\ldots,H_{m'}$ are the statements we were looking for, and $E = H_{1'}$.

- $E \equiv \texttt{suspend}\ E'\ \texttt{when}\ s$.
  Since $E' = E_{1'}$ and $=$ is a congruence, we infer $E = \texttt{suspend}\ E_{1'}\ \texttt{when}\ s$.
  By axiom *susp*, we have $\texttt{suspend}\ E_{i'}\ \texttt{when}\ s = E_{i'}^s$, for $E_{i'}^s$ a normal form, and $E_{i'}^s \equiv F_{i',1}^s \,||\ldots||\, F_{i',n_{i'}}^s$, where

$$F_{i',j}^s = \begin{cases} F_{i',j}[K_{i',j}/E_{f(i',j)}] & \text{if } F_{i',j} \equiv \texttt{if}\ \vartheta_{i',j}\ \texttt{then pause};E_{f(i',j)}, \\ F_{i',j} & \text{otherwise,} \end{cases}$$

  where $K_{i',j} \equiv \texttt{if}\ s^+\ \texttt{then pause};K_{i',j}\ ||\ \texttt{if}\ s^-\ \texttt{then}\ E_{f(i',j)}^s$.
  Now, $\texttt{if}\ s^-\ \texttt{then}\ E_{f(i',j)}^s$ can be transformed into a normal form as in the case for $\texttt{present}\ \_\ \texttt{then}\ \_\ \texttt{else}\ \_\ \texttt{end}$, so that $E_{i'}^s$ is transformed into a parallel composition of normal forms, with normal forms as derivatives. Let us call $K_{i'}$ such a statement. Every $K_{i'}$ can be transformed into a normal form $H_{i'}$ as in the case of "||". So, $H_{1'},\ldots H_{m'}$ are the statements we were looking for, and $E = H_{1'}$. □

We introduce now the notion of guarded recursive specification.

A *recursive specification* over variables $\vec{P} = P_1,\ldots,P_m$ is a set of equations

$$P_i = F_i, \quad 1 \leqslant i \leqslant m,$$

where F_i is a statement, $1 \leqslant i \leqslant m$, and it is *guarded* if $P_1,\ldots,P_m$ are guarded in $F_1,\ldots,F_m$. A *solution* is a set of statements $\vec{E} \equiv E_1,\ldots,E_m$ such that $E_i = F_i[\vec{E}/\vec{P}]$, $1 \leqslant i \leqslant m$.

The following lemma states that every guarded recursive specification has a solution, which is unique modulo $=$.

Lemma 45. *Every guarded recursive specification*

$$P_i = F_i, \quad 1 \leqslant i \leqslant m$$

has a solution $\vec{E} \equiv E_1,\ldots,E_m$. *Moreover, given any solution* $\vec{E'} \equiv E'_1,\ldots,E'_m$, *we have* $E'_i = E_i$, $1 \leqslant i \leqslant m$.

Lemma 45 has been proved in [24] for CCS. The proof of [24], which exploits axiom rec_2, can be immediately generalized to Esterel$^+$, as it is shown in [32].

We show now that two arbitrary bisimilar constructive Esterel statements are equated by axioms in Tables 2–8.

Lemma 46. *Given constructive Esterel statements* E *and* E', $E \approx E'$ *implies* $E = E'$.

Proof. By Lemma 44, there exist normal forms $E_1,\ldots,E_m$, $E_{1'},\ldots,E_{m'}$ such that:

- $E=E_1$, $E'=E_{1'}$
- $E_i=F_{i,1}\,||\ldots||\,F_{i,n_i}$, $1\leqslant i\leqslant m$
- $E_{i'}=F_{i',1}\,||\ldots||\,F_{i',n_{i'}}$, $1\leqslant i'\leqslant m'$
- $F_{i,j}\equiv \texttt{if}\ \vartheta_{i,j}\ \texttt{then}\ G_{i,j}$, $1\leqslant i\leqslant m$, $1\leqslant j\leqslant n_i$
- $F_{i',j'}\equiv \texttt{if}\ \vartheta_{i',j'}\ \texttt{then}\ G_{i',j'}$, $1\leqslant i'\leqslant m'$, $1\leqslant j'\leqslant n_{i'}$.

So, to prove the thesis it is sufficient to prove that $E_1=E_{1'}$.

Let us denote by $\mathscr{I}\subseteq\{1,\ldots,m\}\times\{1',\ldots,m'\}$ the set of pairs (i,i') such that $E_i\approx E_{i'}$. Since $E\approx E'$, $E=E_1$ and $E'=E_{1'}$, and $=$ is sound modulo $\approx$, we have $(1,1')\in\mathscr{I}$.

We prove now that, given a pair $(i,i')\in\mathscr{I}$, and an index $1\leqslant j\leqslant n_i$, there exists an index $1\leqslant j'\leqslant n_{i'}$ such that:

- $\vartheta_{i',j'}=\vartheta_{i,j}$;
- either $G_{i,j}\equiv G_{i',j'}$ or $G_{i,j}\equiv \texttt{pause};E_{f(i,j)}$, $G_{i',j'}\equiv \texttt{pause};E_{f(i',j')}$ and $(f(i,j),f(i',j'))\in\mathscr{I}$.

We consider the following cases:

- $G_{i,j}\equiv \texttt{emit}\ s$.
  There exists a label l such that $E_i\xrightarrow{l}$ and $\vartheta_{i,j}s\in\mathscr{E}_l$. Since $E_i\approx E_{i'}$, we have $E_{i'}\xrightarrow{l}$. Since $\vartheta_{i,j}s\in\mathscr{E}_l$, there exists $1\leqslant j'\leqslant n_{i'}$ such that $\vartheta_{i',j'}=\vartheta_{i,j}$ and $G_{i',j'}\equiv\texttt{emit}\ s$.
- $G_{i,j}\equiv\texttt{nothing}$.
  Since E_i is a normal form and, in particular, it satisfies Conditions 4 and 5 of Definition 36, there exists a label l such that $E_i\xrightarrow{l}$ and $\vartheta_{i,j}n\in\mathscr{E}_l$. Since $E_i\approx E_{i'}$, we have $E_{i'}\xrightarrow{l}$. Since $\vartheta_{i,j}n\in\mathscr{E}_l$, there exists $1\leqslant j'\leqslant n_{i'}$ such that $\vartheta_{i',j'}=\vartheta_{i,j}$ and $G_{i',j'}\equiv\texttt{nothing}$.
- $G_{i,j}\equiv\texttt{exit}\ T$.
  There exists a label l such that $E_i\xrightarrow{l}$ and $\vartheta_{i,j}T\in\mathscr{E}_l$. Since $E_i\approx E_{i'}$, we have $E_{i'}\xrightarrow{l}$. Since $\vartheta_{i,j}T\in\mathscr{E}_l$, there exists $1\leqslant j'\leqslant n_{i'}$ such that $\vartheta_{i',j'}=\vartheta_{i,j}$ and $G_{i',j'}\equiv\texttt{exit}\ T$.
- $G_{i,j}\equiv\texttt{pause}$ and $|\vartheta_{i,j}|\cap\{s^+,s^-\}=\emptyset$ for some $s\in\mathscr{S}$.
  Since E_i is a normal form and, in particular, it satisfies Condition 4 of Definition 36, there exists a label l such that $E_i\xrightarrow{l}$ and $\vartheta_{i,j}p\in\mathscr{E}_l$. Since $E_i\approx E_{i'}$, we have $E_{i'}\xrightarrow{l}$. Since $\vartheta_{i,j}p\in\mathscr{E}_l$, there exists $1\leqslant j'\leqslant n_{i'}$ such that $\vartheta_{i',j'}=\vartheta_{i,j}$ and $G_{i',j'}\equiv\texttt{pause}$.
- $G_{i,j}\equiv\texttt{pause};E_{f(i,j)}$.
  Since E_i is a normal form and, in particular, it satisfies Conditions 2 and 3 of Definition 36, there exists a label l such that $E_i\xrightarrow{l}\texttt{nothing}\,||\ldots||\,\texttt{nothing};E_{f(i,j)}||\ldots||\,\texttt{nothing}$.
  Since $E_i\approx E_{i'}$, we have $E_{i'}\xrightarrow{l}\texttt{nothing}\,||\ldots||\,\texttt{nothing};E_{f(i',j')}\,||\ldots||\,\texttt{nothing}$ and $E_{f(i,j)}\approx E_{f(i',j')}$, for some $1\leqslant j'\leqslant n_{i'}$ such that $G_{i',j'}\equiv\texttt{pause};E_{f(i',j')}$ and $|\vartheta_{i,j}|=|\vartheta_{i',j'}|$.
  Let us assume that $\vartheta_{i,j}\neq\vartheta_{i',j'}$. Now, if $\vartheta_{i,j}p\in\mathscr{E}_l$ then there exists $1\leqslant h'\leqslant n_{i'}$ such that $F_{i',h'}\equiv\texttt{if}\ \vartheta_{i,j}\ \texttt{then pause}$. By axioms $||_3$, seq_3 and $||_7$ we infer $\texttt{if}\ \vartheta_{i',j'}\ \texttt{then pause};E_{f(i',j')}\,||\,\texttt{if}\ \vartheta_{i',h'}\ \texttt{then pause}=\texttt{if}\ \vartheta_{i',j'}\ \texttt{then pause}||\texttt{if}\ \vartheta_{i',h'}\ \texttt{then pause};E_{f(i',j')}$, and we repeat our reasoning. If $\vartheta_{i,j}p\notin\mathscr{E}_l$, then there exists $1\leqslant k\leqslant n_i$ such that $\vartheta_{i,j}=\vartheta_{i,k}\phi$, for some $\phi\in(\mathscr{S}^+_-)^*$, and such that $G_{i,k}\equiv\texttt{pause}$. Since $\vartheta_{i,k}p\in\mathscr{E}_l$,

there exists $1 \leqslant k' \leqslant n_{i'}$ such that $G_{i',k'} \equiv \texttt{pause}$ and $\vartheta_{i',k'} = \vartheta_{i,k}$. Now, $F_{i',k'} = F_{i',k'} \,||\, \texttt{if } \vartheta_{i,j} \texttt{ then pause}$, by axiom $||_6$. So, we are in the case above.

- $G_{i,j} \equiv \texttt{pause}$ and $|\vartheta_{i,j}| \cap \{s^+, s^-\} \neq \emptyset$ for every $s \in \mathscr{S}$.
  Since E_i is a normal form and, in particular, it satisfies Condition 4 of Definition 36, there exists a label l such that $E_i \xrightarrow{l}$ and $\vartheta_{i,j} p \in \mathscr{E}_l$. Since $E_i \approx E_{i'}$, we have $E_{i'} \xrightarrow{l}$. Since $\vartheta_{i,j} p \in \mathscr{E}_l$, there exists $1 \leqslant j' \leqslant n_{i'}$ such that $\vartheta_{i',j'} = \vartheta_{i,j}$ and either $G_{i',j'} \equiv \texttt{pause}$, or $G_{i',j'} \equiv \texttt{pause}; E_{f(i',j')}$. In the first case the thesis is proved. In the second case, there exists a parallel component $\texttt{if } \vartheta_{i,k} \texttt{ then pause}; E_{f(i,k)}$, $1 \leqslant i \leqslant k$, with $E_{f(i,k)} \approx E_{f(i',j')}$, for what we have proved in the case above. But this is impossible, by Condition 6 of Definition 36.

Let us consider now the recursive specification

$$P_{i,i'} = E_{i,i'}, \quad (i,i') \in \mathscr{I},$$

where $E_{i,i'}$ is the statement such that $E_{i,i'} \equiv H_{i,i',1} \,||\, \ldots \,||\, H_{i,i',n_i}$, with either $H_{i,i',j} \equiv \texttt{if } \vartheta_{i,j} \texttt{ then pause}; P_{f(i,j),f(i',j')}$, if $F_{i,j} \equiv \texttt{if } \vartheta_{i,j} \texttt{ then pause}; E_{f(i,j)}$ and $F_{i',j'} \equiv \texttt{if } \vartheta_{i,j} \texttt{ then pause}; E_{f(i',j')}$, or $H_{i,i',j} \equiv F_{i,j} \equiv F_{i',j'}$, otherwise.

This recursive specification is guarded and has both $\vec{G}$ and $\vec{G'}$ as solutions, where $G_{i,i'} \equiv E_i$ and $G'_{i,i'} \equiv E_{i'}$ for each $(i,i') \in \mathscr{I}$. Now, by Lemma 45 it follows that $E_i = E_{i'}$, $(i,i') \in \mathscr{I}$. Since $(1,1') \in \mathscr{I}$, we have $E_1 = E_{1'}$, as required. □

The following theorem states that axioms in Tables 2–8 give an axiomatization sound and complete modulo bisimulation on constructive statements.

Theorem 47. *Given constructive Esterel statements E and E', $E = E'$ if and only if $E \approx E'$.*

Proof. "If": by Lemma 46. "Only if": by Lemma 43. □

5. Correspondence between LTS and circuit semantics

In this section we prove that our LTS semantics agrees with the circuit semantics given in [11]. In Section 5.1, we recall the circuit semantics and in Section 5.2 we show that our LTS carries all information which is needed both to establish whether circuits corresponding to statements are constructive according to [30], and to recover their input/output behavior.

5.1. The circuit semantics

The circuit semantics maps each Esterel statement to a sequential circuit. This mapping is compositional w.r.to the structure of statements, namely the circuit corresponding to a given statement is obtained as a suitable composition of circuits corresponding to its substatements.

We denote with C_E the circuit implementing the Esterel statement E. A latch in C_E is associated with each occurrence of `pause` in the body of E and is set in correspondence with the execution of the `pause` considered, while other constructs are translated into combinatorial logic. States of C_E (i.e. sets of set latches) correspond to configurations of E, namely to sets of `pause` in which E is pausing. A wire `s` is associated with each signal s and is set when s is present. Circuit one-clock executions correspond to statement reactions.

The input/output interface of circuits is standard. A circuit C_E has a set of input pins `I` corresponding to input signals I, and a set of output pins `O` corresponding to output signals O. A wire $\mathtt{i} \in \mathtt{I}$ is set by the environment in correspondence with the communication of signal i. Analogously, C_E sets a wire $\mathtt{o} \in \mathtt{O}$ in correspondence with the communication of signal o.

The input interface of C_E consists also of pins `GO`, `RES`, `SUSP`, `KILL`, while the output interface consists also of pins `SEL`, $\mathtt{K}_i$, $0 \leqslant i \leqslant |\mathscr{T}| + 1$.

Input pin `GO` is used to activate C_E in correspondence with the starting of E. Input pin `RES` is used to reactivate C_E in correspondence with the resuming of E. Input pin `SUSP` is used to suspend the activity of C_E in correspondence with the suspension of E. Input pin `KILL` is used to unset latches of C_E in correspondence with a trap exit, namely in correspondence with the preemption of E.

Output pin $\mathtt{K}_0$ is set by C_E in correspondence with the termination of E. Output pin $\mathtt{K}_1$ is set by C_E in correspondence with the pausing of E. Output pin $\mathtt{K}_i$, $i \geqslant 2$, is set by C_E in correspondence with the fact that E exits the $(i-1)$th outermost trap. We will refer to $\mathtt{K}_0, \mathtt{K}_1, \ldots$, as the *termination pins* of C_E. If $\mathtt{K}_i$ refers to trap T, we will denote $\mathtt{K}_i$ also with $\mathtt{K}_T$. Finally, pin `SEL` is set by C_E to indicate that E is selected for resumption, namely that some internal latch has been set. Pin `SEL` is simply the orring of all internal latches.

In order to start execution of C_E, pin `GO` is set. At subsequent cycles, pin `RES` is set to resume C_E. At each cycle, control propagates within C_E, so that wires corresponding to output signals are set in correspondence with executions of statements `emit`, a termination wire is set, latches corresponding to executed occurrences of `pause` are set.

To suspend E for an execution cycle, pin `SUSP` is set, instead of pin `RES`. If E is preempted by some internal or concurrent trap exit, then pin `KILL` is set to unset latches.

The wire `SEL` is propagated upwards in compound statements and it remains set as long as some latch is set. The wire `SEL` is necessary since `RES` may also be sent to currently unselected statements. When `RES` is set, unselected statements do not react. This is implemented by adding `RES` and `SEL`.

We explain now the general idea of the construction of circuit C_E corresponding to statement E.

- $E \equiv$ `nothing`: pin `GO` is connected to pin $\mathtt{K}_0$. This implements the immediate termination of E.
- $E \equiv$ `emit` s: pin `GO` is connected both to pin $\mathtt{K}_0$ and to output pin `s`. So, when E starts, it sets signal s to "present" and it terminates immediately.

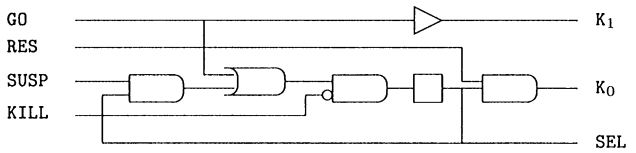

Fig. 1. The circuit for statement pause.

- $E \equiv$ pause: the circuit implementing E is described in Fig. 1. Pin GO is connected to pin K_1, as E pauses when it is started. The latch is set when KILL is not set and either GO is set or both SEL and SUSP are set. So, if E is preempted by some trap exit then the latch is unset. Otherwise, the latch is set when E is started or when E is both selected for resumption and suspended. In the second case, E is in the body of a statement suspend. Output pin K_0 is set when both the latch and RES are set. This means that E terminates when it is resumed after the pausing.
- $E \equiv$ present s then E_1 else E_2 end: input pins s and GO of C_E are anded and the result is connected to pin GO of C_{E_1}, so that E_1 is started only if s is present. Pin GO of C_E and the negation of input pin s of C_E are anded and the result is connected to pin GO of C_{E_2}, so that E_2 is started only when s is absent. Input pins I, KILL, RES and SUSP of C_E are connected to the respective pins of C_{E_1} and C_{E_2}, since if E_i is activated then it views the same input interface of E and it is preempted, resumed and suspended when E is, $1 \leqslant i \leqslant 2$. Output pins of C_E are obtained by orring the respective output pins of C_{E_1} and C_{E_2}. In fact, E terminates, pauses, exits a trap and emits a signal iff either E_1 or E_2 does it.
- $E \equiv E_1 \parallel E_2$: all input pins of C_E are connected to the respective input pins of C_{E_1} and C_{E_2}. This corresponds to the fact that E_1 and E_2 run synchronously and view the same input interface. Output pins of C_E but termination pins are obtained as orring of the respective output pins of C_{E_1} and C_{E_2}. A logic synchronizer sets output pin K_i of C_E iff either pin K_i of C_{E_1} is set and no pin K_j, with $i<j$, of C_{E_2} is set, or conversely. This means that E terminates iff both E_1 and E_2 terminate, E exits the trap T iff T is the outermost trap exited by E_1 and E_2, E pauses iff either E_1 pauses and E_2 does not exit any trap, or conversely.
- $E \equiv E_1;\ E_2$: input pin GO of C_E is connected to pin GO of C_{E_1}, so that the starting of E coincides with the starting of E_1. Output pin K_0 of C_{E_1} is connected to input pin GO of C_{E_2}, so that E_2 starts when E_1 terminates. Output pin K_0 of C_{E_2} is connected to pin K_0 of C_E, so that E terminates when E_2 terminates. Input pins I, KILL, RES and SUSP of C_E are connected to the respective pins of C_{E_1} and C_{E_2}, since if E_i is activated then it views the same input interface of E and it is preempted, resumed and suspended when E is. Output pins SEL, O and K_i, $i \geqslant 1$, of C_E are obtained as orring of the respective output pins of C_{E_1} and C_{E_2}. In fact, E pauses, exits a trap and emits a signal iff either E_1 or E_2 does it.
- $E \equiv$ signal s in E_1 end: C_E is obtained from C_{E_1} by connecting output pin s to input pin s. Cycles of wires may be created.

- $E \equiv$ `loop` E_1 `end`: since E executes infinitely E_1, it would seem to be natural to connect pin $\mathtt{K}_0$ of C_{E_1} to pin `GO` of C_{E_1}, so that C_{E_1} is reactivated in correspondence with the restarting of E_1. This solution is rejected in [11] because it originates *schizophrenia*. Namely, if E_1 may terminate in the cycle subsequent that of its starting, it may happen that cycles of wires internal to C_E do not stabilize electrically. A possible solution is to duplicate the body of a `loop`, namely to replace `loop` E_1 `end` by `loop` $E_1; E_1$ `end`. In fact, schizophrenia cannot arise if the body of a `loop` needs at least two reactions to terminate. Here, we assume that this solution to schizophrenia is adopted, namely we assume that the body of a `loop` is of the form $F;F$, where F cannot terminate immediately. In [11] a more efficient solution is adopted. Bodies of statements `loop` are not duplicated, and a suitable duplication of the circuit logic solves schizophrenia. Resulting circuits are equivalent to those obtained by duplicating bodies of `loop`.
- $E \equiv$ `suspend` E_1 `when` s: since E_1 cannot be suspended at the first execution cycle, pin `GO` of C_E is connected to pin `GO` of C_{E_1}. The anding of pins `SEL` of C_{E_1}, `RES` of C_E and of the negation of pin `s` of C_E is connected to pin `RES` of C_{E_1}, so that E_1 is resumed when it is selected for resumption and s is absent. The anding of pins `SEL` of C_{E_1}, `RES` of C_E and `s` of C_E is connected to pin `SUSP` of C_{E_1}, so that E_1 is suspended when it is selected for resumption and s is present. Input wires `I` of C_E are connected to the corresponding wires of C_{E_1}. Output wires `O` and $\mathtt{K}_i$, $i \geqslant 0$, of C_{E_1} are connected to the corresponding wires of C_E.
- $E \equiv$ `trap` T `in` E_1 `end`: Input pins of C_E but `KILL` are connected to the respective pins of C_{E_1}. Pin `KILL` of C_E and pin $\mathtt{K}_2$ (i.e. pin $\mathtt{K}_T$) of C_{E_1} are composed in or and the result is connected to pin `KILL` of C_{E_1}, so that latches of C_{E_1} are unset when either E_1 exits the trap T or when the latches of C_E must be unset. As E terminates when E_1 either terminates or exits trap T, then the orring of pins $\mathtt{K}_0$ and $\mathtt{K}_2$ of C_{E_1} is connected to pin $\mathtt{K}_0$ of C_E. As E pauses when E_1 pauses, pin $\mathtt{K}_1$ of E_1 is connected to pin $\mathtt{K}_1$ of E. As E exits the ith outermost trap if E_1 exits the $(i+1)$th outermost trap, then pin $\mathtt{K}_{i+1}$ of C_{E_1} is connected to pin $\mathtt{K}_i$ of C_E, for $i \geqslant 2$.
- $E \equiv$ `exit` T: let i be the cardinality of the set of trap declarations of the form `trap` T' `in` $E_{T'}$ `end` such that:
  - `exit` T is in the body of `trap` T';
  - declaration `trap` T' is in the body of `trap` T.

  Then pin `GO` of C_E is connected to pin $\mathtt{K}_{i+2}$ of C_E.

Given a module M, we denote with E_M its body and with C_M the circuit corresponding to M. Circuit C_M is obtained by connecting a so called *boot latch* to pin `GO` of C_{E_M}. This latch is set only at the first execution cycle, so that C_{E_M} is activated only at the first execution cycle. Input pin `RES` of C_{E_M} is always set, so that C_{E_M} is resumed at each execution cycle. Note that, since `SEL` is unset at the first execution cycle, the fact that `RES` is set does not affect the behavior of C_{E_M}. Input pins `I` of C_{E_M} are set by the environment at each execution cycle. Finally, input pins `KILL` and `SUSP` of C_{E_M} are never set.

Causality between signals, reactivity, determinism and constructiveness of statements have a physical interpretation. Signal causality in E corresponds to wire connections in C_E. In fact, if a statement `emit` s is in the `then` branch of statements "`present` s_1",..., "`present` s_n" and in the `else` branch of statements "`present` s_{n+1}",..., "`present` s_m", then the anding of the wires $\mathtt{s}_1,\ldots,\mathtt{s}_n$ and of the negation of the wires $\mathtt{s}_{n+1},\ldots,\mathtt{s}_m$ is connected to `s`.

Now, according to [30] a circuit is *constructive in a reachable state* if and only if it electrically stabilizes for any input, and a circuit is *constructive* if and only if it is constructive in any reachable state. A statement E is reactive, deterministic and constructive if and only if the circuit C_E is constructive. As an example, in the circuit corresponding to statement

`signal` s `in (present` s `then emit` s `else emit` s `end) end`

of Example 23, the orring of the wire `s` and of its negation is connected to `s` itself, so that this wire cannot stabilize and the circuit is nonconstructive.

5.2. The proof of correspondence

We show now that the information carried by LTS labels permits to deduce how output wires of a circuit stabilize electrically when the electrical value at which input wires stabilize is known.

Lemma 48. *Given a transition* $E \xrightarrow{l} F$, *when* C_E *is activated* (*i.e. wire* `GO` *is set*) *the following facts follow*:

(1) *if* $\vartheta o \in \mathscr{E}_l \cup \mathscr{N}_l$, $o \in O$, *each input wire* `i` *such that* $i^+ \in |\vartheta|$ *is kept stable at* 1 *and each input wire* `i` *such that* $i^- \in |\vartheta|$ *is kept stable at* 0, *then the output wire* `o` *stabilizes at* 1;

(2) *if* $\vartheta_1 o,\ldots,\vartheta_v o$ *are the causality terms in* $\mathscr{E}_l \cup \mathscr{N}_l$ *having* o *as action*, $o \in O$, *and, for each* $1 \leqslant j \leqslant v$, *either an input wire* $\mathtt{i}_j$ *such that* $i_j^+ \in |\vartheta_j|$ *is kept stable at* 0 *or an input wire* $\mathtt{i}_j$ *such that* $i_j^- \in |\vartheta_j|$ *is kept stable at* 1, *then the output wire* `o` *stabilizes at* 0;

(3) *if each input wire* `i` *such that* $i^+ \in S_l$ *is kept stable at* 1 *and each input wire* `i` *such that* $i^- \in S_l$ *is kept stable at* 0, *then an output wire* `o`, $o \in O$, *stabilizes at* 1 *if* $o \in Em(l)$, *while it stabilizes at 0 if* $o \notin Em(l)$;

(4) *if each input wire* `i` *such that* $i^+ \in S_l$ *is kept stable at* 1 *and each input wire* `i` *such that* $i^- \in S_l$ *is kept stable at* 0, *then we have that*:
   (a) *if* $\mathscr{T}_l = 0$ *then the termination wire* $\mathtt{K}_0$ *stabilizes at* 1;
   (b) *if* $\mathscr{T}_l = 1$ *then the termination wire* $\mathtt{K}_1$ *stabilizes at* 1;
   (c) *if* $\mathscr{T}_l \subseteq \mathscr{T}$ *then the termination wire* $\mathtt{K}_T$ *stabilizes at* 1, *where* T *is the outermost trap in* $\mathscr{T}_l$.

Proof. We prove facts 1, 2 and 4 by structural induction on E. Facts 1 and 2 imply fact 3.

Base case: If $E \equiv emit\ o$ then we have $E \xrightarrow{l} nothing$, with $l = \langle \emptyset, \{\varepsilon o\}, \emptyset, 0 \rangle$. Since the output wire o and the termination wire $\mathtt{K}_0$ of C_E stabilize at 1, the thesis follows. The proof for the other basic statements is analogous.

Induction step: We must consider the following cases.

- $E \equiv \mathtt{present}\ s\ \mathtt{then}\ E_1\ \mathtt{else}\ E_2\ \mathtt{end}$.

  By rules *present_1* and *present_2*, if $E \xrightarrow{l} F$ then there exist transitions $E_1 \xrightarrow{l_1} F_1$ and $E_2 \xrightarrow{l_2} F_2$ such that either $l = s^+(l_1, l_2)$ and $F \equiv F_1$, or $l = s^-(l_2, l_1)$ and $F \equiv F_2$.
  Let us prove fact 1. By definition of $s^+(l_1, l_2)$ and $s^-(l_2, l_1)$, if $\vartheta o \in \mathscr{E}_l \cup \mathscr{N}_l$ then either $\vartheta = s^+\phi$ and $\phi o \in \mathscr{E}_{l_1} \cup \mathscr{N}_{l_1}$, or $\vartheta = s^-\phi$ and $\phi o \in \mathscr{E}_{l_2} \cup \mathscr{N}_{l_2}$. We assume the first case. The other is analogous. By inductive hypothesis on E_1, if C_{E_1} is activated and each input wire i such that $i^+ \in |\phi|$ (resp. $i^- \in |\phi|$) is kept stable at 1 (resp. 0) then the output wire o of C_{E_1} stabilizes at 1. Now, since s is kept stable at 1 and C_E is activated, then C_{E_1} is activated. It follows that the output wire o of C_{E_1} stabilizes at 1. This wire is connected, through an or-gate, to the output wire o of C_E, which stabilizes at 1.
  Fact 2 follows by inductive hypothesis on E_1 and E_2 and by the fact that the output wire o of C_E is obtained as orring of the output wires o of C_{E_1} and C_{E_2}.
  To prove fact 4, let us assume that $l = s^+(l_1, l_2)$. The other case is analogous. The thesis follows by inductive hypothesis on E_1, by the fact that if s stabilizes at 1 and C_E is activated then C_{E_1} is activated, by the fact that wire $\mathtt{K}_i$ of C_{E_1} is connected, through an or-gate, to wire $\mathtt{K}_i$ of C_E, $i \geqslant 0$, and by the fact that $\mathscr{T}_l = \mathscr{T}_{l_1}$.
- $E \equiv E_1 \parallel E_2$.

  By rules *parallel_1* and *parallel_2*, if $E \xrightarrow{l} F$ then there exist transitions $E_1 \xrightarrow{l_1} F_1$ and $E_2 \xrightarrow{l_2} F_2$ such that $l = l_1 \otimes l_2$.
  Facts 1 and 2 follow by inductive hypothesis on E_1 and E_2, by the fact that when C_E is activated then both C_{E_1} and C_{E_2} are activated, and by the fact that the output wire o of C_E is obtained as orring of the output wires o of C_{E_1} and C_{E_2}.
  Fact 4 follows directly by inductive hypothesis on E_1 and E_2 and by the definition of $\mathscr{T}_{l_1 \otimes l_2}$.
- $E \equiv E_1; E_2$.

  By rules *seq_1*, *seq_2* and *seq_3*, if $E \xrightarrow{l} F$ then there exist transitions $E_1 \xrightarrow{l_1} F_1$ and $E_2 \xrightarrow{l_2} F_2$ such that $l = l_1 \rhd l_2$ and either $\mathscr{T}_{l_1} = 0$ and $F \equiv F_2$, or $\mathscr{T}_{l_1} = 1$ and $F \equiv F_1; E_2$, or $\mathscr{T}_{l_1} \subseteq \mathscr{T}$ and $F \equiv \mathtt{nothing}$.
  Let us prove fact 1. If $\vartheta o \in \mathscr{E}_l \cup \mathscr{N}_l$ then either $\vartheta o \in \mathscr{E}_{l_1} \cup \mathscr{N}_{l_1}$, or $\vartheta = \phi\vartheta'$, $\phi \in \mathscr{I}(E_1)$ and $\vartheta' o \in \mathscr{E}_{l_2} \cup \mathscr{N}_{l_2}$. In the first case, since the activation of C_E implies the activation of C_{E_1}, the output wire o of C_{E_1} stabilizes at 1 by inductive hypothesis on E_1. Since this wire is connected, through an or-gate, to the output wire o of C_E, fact 1 follows. In the second case, since by inductive hypothesis on E_2 if each wire i with $i^+ \in |\vartheta'|$ (resp. $i^- \in |\vartheta'|$) stabilizes at 1 (resp. 0) then the output wire o of C_{E_2} stabilizes at 1, and this wire is connected, through an or-gate, to the output wire o of C_E, we must prove that C_{E_2} is activated. This happens since, by inductive hypothesis on E_1 (fact 4), if each input wire i with $i^+ \in |\phi|$ (resp. $i^- \in |\phi|$) stabilizes at 1 (resp. 0),

and $\phi \in \mathscr{I}(E_1)$, then the wire $\mathtt{K}_0$ of C_{E_1} stabilizes at 1. Now, this wire is connected to the wire GO of C_{E_2}.

Fact 2 follows by inductive hypothesis on E_1 and E_2, and by the fact that the output wire o of C_E is obtained as orring of the output wires o of C_{E_1} and C_{E_2}.

If $\mathscr{T}_l \neq 0$ then fact 4 follows by inductive hypothesis on E_1. If $\mathscr{T}_l = 0$ then fact 4 follows by inductive hypothesis on E_2.

- $E \equiv \mathtt{signal}\ s\ \mathtt{in}\ E'\ \mathtt{end}$.

  By rule *signal*, if $E \xrightarrow{l} F$ then there exists a transition $E' \xrightarrow{l'} F'$ such that $F \equiv \mathtt{signal}\ s\ \mathtt{in}\ F'\ \mathtt{end}$ and $l = loc(s, l')$.

  Let us prove fact 1. If $\vartheta o \in \mathscr{E}_l \cup \mathscr{N}_l$ then, by definition of function *loc*, a causality term $\vartheta' o$ is in $\mathscr{E}_{l'} \cup \mathscr{N}_{l'}$ and one of the following cases holds:
  - $\vartheta = \vartheta'$: fact 1 follows by inductive hypothesis.
  - $\vartheta = \vartheta'[\phi/s^+]$: fact 1 follows by inductive hypothesis if we prove that, when each wire i such that $i^+ \in |\phi|$ stabilizes at 1 and each wire i such that $i^- \in |\phi|$ stabilizes at 0, then s stabilizes at 1. Now, this property follows by inductive hypothesis (fact 1), since, by definition of function *loc*, there exists a causality term $\phi s \in \mathscr{E}_{l'} \cup \mathscr{N}_{l'}$.
  - $\vartheta = \vartheta'[\phi/s^-]$: fact 1 follows by inductive hypothesis if we prove that, when each wire i such that $i^+ \in |\phi|$ stabilizes at 1 and each wire i such that $i^- \in |\phi|$ stabilizes at 0, then s stabilizes at 0. Now, this property follows by inductive hypothesis (fact 2), since, by definition of function *loc*, given $\phi_1 s, \ldots, \phi_m s$ the causality terms in $\mathscr{E}_{l'} \cup \mathscr{N}_{l'}$ having s as action, $\phi_i = \gamma_{i,1} \ldots \gamma_{i,n_i}$, we have that $\phi = \gamma_{i_1,1} \ldots \overline{\gamma_{i_1,j_{i_1}}} \ldots \gamma_{i_m,1} \ldots \overline{\gamma_{i_m,j_{i_m}}}$.

  Let us prove fact 2. If $\vartheta_1 o, \ldots, \vartheta_v o \in \mathscr{E}_l \cup \mathscr{N}_l$ then, by definition of function *loc*, there exist causality terms $\vartheta'_1 o, \ldots, \vartheta'_m o \in \mathscr{E}_{l'} \cup \mathscr{N}_{l'}$ and we have that $\vartheta_1, \ldots, \vartheta_v = \vartheta_{(1,1)}, \ldots, \vartheta_{(1,k_1)}, \ldots, \vartheta_{(m,1)}, \ldots, \vartheta_{(m,k_m)}$. By inductive hypothesis, the thesis follows if we prove that, for each $1 \leqslant j \leqslant m$, there exists a wire $\mathtt{i}'_j$ which stabilizes at 0 (resp. 1) and $i'^+_j \in |\vartheta'_j|$ (resp. $i'^-_j \in |\vartheta'_j|$).

  For each $1 \leqslant j \leqslant m$ we have one of the following cases.
  - $\vartheta_{(j,1)} = \vartheta'_j$ and $k_j = 1$: in this case we can take $\mathtt{i}'_j = i_{(j,1)}$.
  - $\vartheta_{(j,h)} = \vartheta'_j[\phi_h/s^+]$, where $\phi_h s \in \mathscr{E}_{l'} \cup \mathscr{N}_{l'}$, $1 \leqslant h \leqslant k_j$. Now, if $i_{(j,h)} \notin |\phi_h|$ for some h then we take $\mathtt{i}'_j = i_{(j,h)}$. Otherwise, if $i_{(j,h)} \in \phi_h$ for each h then s stabilizes at 0 by inductive hypothesis (fact 2) and we take $\mathtt{i}'_j = \mathtt{s}$.
  - $\vartheta_{(j,h)} = \vartheta'_j[\phi_h/s^-]$, where for $\psi_1 s, \ldots, \psi_m s$ the causality terms in $\mathscr{E}_{l'} \cup \mathscr{N}_{l'}$ having s as action, $\psi_i = \gamma_{i,1} \ldots \gamma_{i,n_i}$, we have that $\phi_h = \gamma_{i_1,1}, \ldots, \overline{\gamma_{i_1,j_{i_1}}} \ \ldots \ \ldots \gamma_{i_m,1} \ldots \overline{\gamma_{i_m,j_{i_m}}}$. If $i_{(j,h)} \notin |\phi_h|$ for some h then we take $\mathtt{i}'_j = \mathtt{i}_{(j,h)}$. Otherwise, if $i_{(j,h)} \in \phi_h$ for each h, then s stabilizes at 1 by inductive hypothesis (fact 1) and we take $\mathtt{i}'_j = \mathtt{s}$.

  Since $\mathscr{T}_l = \mathscr{T}_{l'}$, and wire $\mathtt{K}_i$ of $C_{E'}$ is connected to wire $\mathtt{K}_i$ of C_E, fact 4 follows by inductive hypothesis if we prove that each input wire i such that $i^+ \in S_{l'}$ stabilizes at 1 and each input wire i such that $i^- \in S_{l'}$ stabilizes at 0. Now, by definition of *loc*, $S_l = S_{l'} \setminus \{s^-, s^+\}$. So, if $s^+ \in S_{l'}$ then we must prove that s stabilizes at 1, while if $s^- \in S_{l'}$ then we must prove that s stabilizes at 0. If $s^+ \in S_{l'}$ then there

exists a causality term $\vartheta s \in \mathscr{E}_{l'}$ with $|\vartheta| \subseteq S_l$. So, by inductive hypothesis on E' (fact 1), if each wire `i` such that $i^+ \in S_l$ stabilizes at 1 and each wire `i` such that $i^- \in S_l$ stabilizes at 0 then `s` stabilizes at 1. If $s^- \in S_{l'}$ then, given $\psi_1 s, \ldots, \psi_m s$ the causality terms in $\mathscr{N}_{l'}$ with s as action, $\psi_i = \gamma_{i,1} \ldots \gamma_{i,n_i}$, then $|\gamma_{1,1} \ldots \overline{\gamma_{1,j_1}} \ldots \gamma_{m,1} \ldots \overline{\gamma_{m,j_m}}| \subseteq S_l$. So, by inductive hypothesis on E' (fact 2), if each wire `i` such that $i^+ \in S_l$ stabilizes at 1 and each wire `i` such that $i^- \in S_l$ stabilizes at 0 then `s` stabilizes at 0.

- $E \equiv$ `loop` E' `end`.

  By rules *loop_1* and *loop_2*, if $E \xrightarrow{l} F$ then there exists a transition $E' \xrightarrow{l} F'$ such that either $F \equiv F'; E$ and $\mathscr{T}_l = 1$, or $F \equiv$ `nothing` and $\mathscr{T}_l \subseteq \mathscr{T}$. Facts 1 and 2 follow by inductive hypothesis on E'. Fact 4 follows by the fact that $\mathscr{T}_l = \mathscr{T}_{l'}$, the inductive hypothesis on E' and by the fact that each wire $\mathtt{K}_i$, $i \geqslant 1$, of $C_{E'}$ is connected to the wire $\mathtt{K}_i$ of C_E.
- $E \equiv$ `trap` T `in` E' `end`.

  By rules *trap_1*, *trap_2*, *trap_3*, if $E \xrightarrow{l} F$ then there exists a transition $E' \xrightarrow{l'} F'$ such that either $\mathscr{T}_{l'} \in \{0, \{T\}\}$ and $\mathscr{T}_l = 0$, or $\mathscr{T}_{l'} = 1 = \mathscr{T}_l$, or $\mathscr{T}_{l'} \subseteq \mathscr{T}$, $\mathscr{T}_{l'} \neq \{T\}$ and $\mathscr{T}_l = \mathscr{T}_{l'} \setminus \{T\}$. Facts 1 and 2 follow by inductive hypothesis. If $\mathscr{T}_{l'} = 0$ or $\mathscr{T}_{l'} = \{T\}$ then fact 4 follows by the inductive hypothesis and the fact that the wire $\mathtt{K}_0$ of C_E is obtained by orring the wires $\mathtt{K}_0$ and $\mathtt{K}_T$ of $C_{E'}$. If $\mathscr{T}_{l'} = 1$, then fact 4 follows by the inductive hypothesis and the fact that the wire $\mathtt{K}_1$ of $C_{E'}$ is connected to the wire $\mathtt{K}_1$ of C_E. If $\mathscr{T}_{l'} \subseteq \mathscr{T}$, $\mathscr{T}_{l'} \neq \{T\}$, then fact 4 follows by the inductive hypothesis and the fact that the wire $\mathtt{K}_{T'}$ of $C_{E'}$ is connected to the wire $\mathtt{K}_{T'}$ of C_E, for every $T' \not\equiv T$.
- $E \equiv$ `suspend` E' `when` s.

  The thesis follows immediately by inductive hypothesis. □

By Lemma 48 (facts 3 and 4) it follows that if a statement E is constructive according to Definition 28, then the circuit C_E is constructive in its initial state. In fact, given an arbitrary value at which input wires stabilize, all output wires stabilize. We prove now that if E is nonconstructive then C_E is nonconstructive in its initial state.

Lemma 49. *Given a statement E and an input event S_I such that $E \not\xrightarrow{l}$ for any label l such that $S_l \uparrow S_I$, when each input wire* `i` *such that $i^+ \in S_I$ is kept stable at* 1 *and each input wire* `i` *such that $i^- \in S_I$ is kept stable at* 0*, then some wire in C_E does not stabilize electrically.*

Proof. By structural induction over E.

Base case: If E is a basic statement then, by rules in Table 1, we have $E \xrightarrow{l}$ `nothing` and $S_l = \emptyset$. So, $S_I \uparrow S_l$ for any input event S_I, and the thesis follows immediately.

Induction step: The only nontrivial case is that with $E \equiv$ `signal` s `in` E' `end`. Assume first that there are transitions $E' \xrightarrow{l'_1}$ and $E' \xrightarrow{l'_2}$ such that $S_{l'_1} \uparrow S_I \cup \{s^+\}$ and $S_{l'_2} \uparrow S_I \cup \{s^-\}$ (the two transitions may coincide). Given a transition $E' \xrightarrow{l'} F'$, there is no $\vartheta s \in \mathscr{E}_{l'} \cup \mathscr{N}_{l'}$ such that $|\vartheta| \uparrow S_I$ and $|\vartheta| \cap \{s^+, s^-\} = \emptyset$ (i.e. $|\vartheta| \subseteq S_I$). Otherwise,

$\vartheta s \in \mathscr{E}_{l'_1}$ and $loc(s, l'_1)$ is defined, contrarily to the hypothesis. Moreover, there is at least a causality term ϑs with $|\vartheta| \uparrow S_I$ and $|\vartheta| \cap \{s^+, s^-\} \neq \emptyset$. Otherwise, all ϑs in $\mathscr{E}_{l'_2} \cup \mathscr{N}_{l'_2}$ are in $\mathscr{N}_{l'_2}$ and $loc(s, l'_2)$ is defined, contrarily to the hypothesis. So, there are causality terms $\vartheta_1 s, \ldots, \vartheta_v s$ such that $|\vartheta_i| \uparrow S_I$ and $|\vartheta_i| \cap \{s^-, s^+\} \neq \emptyset$, for $1 \leqslant i \leqslant u$, and $|\vartheta_i| \not\uparrow S_I$, for $u+1 \leqslant i \leqslant v$. Assume that input wires of C_E stabilize as stated in the hypothesis. By Lemma 48, the output wire s of $C_{E'}$ stabilizes at 1 if the input wire s stabilizes at 1 (resp. 0) and s^+ (resp. s^-) appears in some ϑ_i, for $1 \leqslant i \leqslant u$. Moreover, the output wire s stabilizes at 0 if for every $1 \leqslant i \leqslant u$, either s^- appears in ϑ_i and the input wire s stabilizes at 1, or s^+ appears in ϑ_i and s stabilizes at 0. So, if the electrical value at which the input wire s is unknown, we cannot deduce the electrical value at which the output wire s stabilizes. Since in C_E the output wire s of $C_{E'}$ is connected to the input wire s of $C_{E'}$, it follows that the obtained loop cannot stabilize electrically.

Assume now that $E' \xrightarrow{l'}$ with $s^- \in S_{l'}$ and $S_{l'} \uparrow S_I$, and that $E' \not\xrightarrow{l''}$ for any l'' such that $s^+ \in S_{l''}$ and $S_{l''} \uparrow S_I$. In this case, the inductive hypothesis implies that if s stabilizes at 1 and input wires stabilizes as assumed by S_I, then some wire internal to $C_{E'}$ does not stabilize. Now, if there is a causality term $\vartheta s \in \mathscr{E}_{l'}$ with $|\vartheta| \subseteq S_I$, so that s stabilizes at 1 by Lemma 48, some wire of $C_{E'}$ does not stabilize and the thesis follows. If no $\vartheta s \in \mathscr{E}_{l'}$ with $|\vartheta| \subseteq S_I$, since $loc(s, l')$ is not defined, there is at least a causality term $\vartheta s \in \mathscr{E}_{l'} \cup \mathscr{N}_{l'}$ with $|\vartheta| \uparrow S_I$ and $|\vartheta| \cap \{s^+, s^-\} \neq \emptyset$. So, we can reason as in the case above and the thesis follows.

Assume now that $E' \xrightarrow{l'}$ with $s^+ \in S_{l'}$ and $S_{l'} \uparrow S_I$, and that $E' \not\xrightarrow{l''}$ for any l'' such that $s^- \in S_{l''}$ and $S_{l''} \uparrow S_I$. Now, there is no causality term $\vartheta s \in \mathscr{E}_{l'}$ with $|\vartheta| \subseteq S_I$, since $loc(s, l')$ is not defined. Since $loc(s, l')$ is not defined, either there is at least a causality term ϑs with $|\vartheta| \uparrow S_I$ and $|\vartheta| \cap \{s^+, s^-\} \neq \emptyset$, so that we can reason as in the first case and the thesis follows, or there is no causality term $\vartheta s \in \mathscr{E}_{l'} \cup \mathscr{N}_{l'}$, so that s stabilizes at 0 by Lemma 48. In this latter case, by the inductive hypothesis some wire in $C_{E'}$ does not stabilize and the thesis follows.

Finally, assume that $E' \not\xrightarrow{l'}$ for any l' with $S_{l'} \uparrow S_I$. In this case, if input wires stabilize as assumed by S_I then some wire of $C_{E'}$ does not stabilize, and the thesis follows. □

Therefore, constructiveness of statements and constructiveness of circuits are related as stated by the following theorem.

Theorem 50. *A statement E is constructive as in Definition* 28 *if and only if the circuit C_E is constructive in its initial state.*

Proof. "If": directly by Lemma 49. "Only if": directly by Lemma 48. □

We show now that the LTS defined in Table 1 carries sufficient information to infer how circuits evolve state by state.

Lemma 51. *Given a constructive statement E and a transition $E \xrightarrow{l} F$ such that $\mathscr{T}_l = 1$, if circuit C_E is activated (i.e. wire* GO *is set) and each input wire* i *such that $i^+ \in S_l$ (resp. $i^- \in S_l$) is kept stable at* 1 (*resp.* 0), *then, when C_E will be resumed, it will behave as C_F.*

Proof. By structural induction over E.

Base case: If $E \equiv \texttt{pause}$ then $F \equiv \texttt{nothing}$. At the next execution cycle, since wire RES and the latch will be set, only the output wire $\texttt{K}_0$ will stabilize at 1. This means that the thesis follows, since when circuit implementing nothing is activated, only the output wire $\texttt{K}_0$ stabilizes at 1. If E is a basic statement and $E \not\equiv \texttt{pause}$, then $\mathscr{T}_l \neq 1$ for every label l such that $E \xrightarrow{l}$, so that the thesis follows immediately.

Induction step: We must consider the following cases.

- $E \equiv \texttt{present}\ s\ \texttt{then}\ E_1\ \texttt{else}\ E_2\ \texttt{end}$.
  By rules *present_1* and *present_2*, if $E \xrightarrow{l} F$ then there exist transitions $E_1 \xrightarrow{l_1} F_1$ and $E_2 \xrightarrow{l_2} F_2$ such that either $l = s^+(l_1, l_2)$ and $F \equiv F_1$, or $l = s^-(l_2, l_1)$ and $F \equiv F_2$. Let us assume the first case. The other is analogous. The thesis follows by inductive hypothesis on E_1 and by the fact that if s stabilizes at 1 then the activation of C_E implies that C_{E_1} is activated and that C_{E_2} is not activated. So, the wire SEL of C_{E_2} will not be set at the following cycle and C_{E_2} will not be selected for resumption.
- $E \equiv E_1 \parallel E_2$.
  By rule *parallel_1*, if $E \xrightarrow{l} F$ with $\mathscr{T}_l = 1$, then there exist transitions $E_1 \xrightarrow{l_1} F_1$ and $E_2 \xrightarrow{l_2} F_2$ such that $l = l_1 \otimes l_2$ and $F = F_1 \parallel F_2$. So, the thesis follows by inductive hypothesis on E_1 and E_2 and by the fact that the activation of C_E implies that both C_{E_1} and C_{E_2} are activated.
- $E \equiv E_1; E_2$.
  By rules *seq_1* and *seq_2*, if $E \xrightarrow{l} F$ with $\mathscr{T}_l = 1$, then there exist transitions $E_1 \xrightarrow{l_1} F_1$ and $E_2 \xrightarrow{l_2} F_2$ such that $l = l_1 \rhd l_2$, and either $\mathscr{T}_{l_1} = 0$, $\mathscr{T}_{l_2} = 1$ and $F \equiv F_2$, or $\mathscr{T}_{l_1} = 1$ and $F \equiv F_1; E_2$. In the first case the thesis follows by inductive hypothesis on E_2, by the fact that the activation of C_E implies that C_{E_1} is activated, and by the fact that Lemma 48 (fact 4) implies that the wire $\texttt{K}_0$ of C_{E_1} stabilizes at 1 so that C_{E_2} is activated. In the second case the thesis follows by inductive hypothesis on E_1, by the fact that the activation of C_E implies that C_{E_1} is activated, by the fact that Lemma 48 (fact 4) implies that the wire $\texttt{K}_0$ of C_{E_1} stabilizes at 0 so that C_{E_2} is not activated.
- $E \equiv \texttt{signal}\ s\ \texttt{in}\ E'\ \texttt{end}$.
  By rule *signal*, if $E \xrightarrow{l} F$ then there exists a transition $E' \xrightarrow{l'} F'$ such that $l = loc(s, l')$ and $F \equiv \texttt{signal}\ s\ \texttt{in}\ F'\ \texttt{end}$. So, the thesis follows by inductive hypothesis on E'.
- $E \equiv \texttt{loop}\ E'\ \texttt{end}$.
  By rule *loop_1*, if $E \xrightarrow{l} F$ with $\mathscr{T}_l = 1$, then there exists a transition $E' \xrightarrow{l} F'$ such that $F \equiv F'; E$. The thesis follows by inductive hypothesis on E' and by the fact that C_E behaves as circuit $C_{E';E}$.
- $E \equiv \texttt{suspend}\ E'\ \texttt{when}\ s$.
  By rule *suspend_2*, if $E \xrightarrow{l} F$ with $\mathscr{T}_l = 1$, then $E' \xrightarrow{l} F'$ and $F \equiv \texttt{suspend imm}\ F'\ \texttt{when}\ s$. The thesis follows since, at the next cycle, if s stabilizes at 1 then the wire $\texttt{K}_1$ of $C_{E'}$ stabilizes at 1, while if s stabilizes at 0 then $C_{E'}$ is resumed and, by inductive hypothesis, it behaves as $C_{F'}$.
- $E \equiv \texttt{trap}\ T\ \texttt{in}\ E'\ \texttt{end}$.

By rule *trap_2*, if $E \xrightarrow{l} F$ with $\mathscr{T}_l = 1$ then there exists a transition $E' \xrightarrow{l'} F'$ such that $F \equiv \texttt{trap}\ T\ \texttt{in}\ F'\ \texttt{end}$ and $l = tr(T, l')$. So, the thesis follows by inductive hypothesis on E'. □

We introduce now the definition of constructiveness of modules.

Definition 52. A *module M* is *constructive* if, for each sequence of transitions $E_0 \xrightarrow{l_1} E_1, \ldots, E_{n-1} \xrightarrow{l_n} E_n$ such that $E_0 \equiv E_M$, statements $E_0, \ldots, E_n$ are constructive.

Note that modules have finite states and their constructiveness is decidable.

Constructiveness of modules as in Definition 52 and constructiveness of circuits are related as stated by the following theorem.

Theorem 53. *A module M is constructive as in Definition* 52 *if and only if the circuit* C_M *is constructive.*

Proof. Directly by Theorem 50 and Lemma 51. □

6. Conclusions

We have presented an axiomatization of the synchronous language Esterel, so to characterize behaviorally equivalent programs.

First of all, we have given a structural operational semantics for Esterel in terms of a labeled transition system, and we have assumed bisimulation as a behavioral equivalence over programs. To justify this assumption, we have proved that bisimulation is a congruence and that our LTS reflects the input/output behavior of programs. Therefore, bisimilar programs are distinguished neither by any Esterel context nor by the external environment.

Then, we have given a system of axioms inducing an axiomatization over Esterel which is sound and complete modulo bisimulation. This axiomatization may be used for program transformation and proof by rewriting.

The axiomatization of Esterel cannot be done by applying classical techniques developed in the field of asynchronous concurrency. Axiomatizations of asynchronous process algebras are based on the transformation of arbitrary processes into "head normal forms". This approach, that stems from [8, 24], has been adopted in [2, 1] to develop algorithmic techniques to compute axiomatizations. In order to transform concurrent processes into head normal forms, concurrency must be simulated by sequentiality plus nondeterminism. This is impossible in the synchronous setting, because programs running in parallel are perfectly synchronized and cannot arbitrarily interleave.

We have proposed a notion of normal form for Esterel programs and we have exploited this notion in the proof of completeness of our axiomatization. A normal form is a parallel composition of programs such that, given an arbitrary input from the

environment, at most one of them does not terminate and will be able to react to the next input.

We believe that our approach could be extended to other state-based synchronous languages, like Argos [23], Statecharts [20] and SyncCharts [4], and constraint based synchronous languages, like Timed Concurrent Constraint Programming [29].

References

[1] L. Aceto, Deriving complete inference systems for a class of GSOS languages generating regular behaviors, in: Proc. CONCUR '94, Lecture Notes in Computer Science, vol. 836, Springer, Berlin, 1994, pp. 449–464.

[2] L. Aceto, B. Bloom, F. Vaandrager, Turning SOS rules into equations, Inform. and Comput. 111 (1994) 1–52.

[3] L. Aceto, W.J. Fokkink, C. Verhoef, Structural operational semantics, To appear in J.A. Bergstra, A. Ponse, S.A. Smolka (Eds.), Handbook of Process Algebra, Elsevier, Amsterdam, 2000.

[4] C. André, Representation and analysis of reactive behaviors: a synchronous approach, Presented at CESA '96, IEEE-SMC, Lille, France, 1996.

[5] A. Benveniste, G. Berry (Eds.), Another look at real-time systems (special issue) Proc. IEEE 79 (1991) 1268–1336.

[6] J.A. Bergstra, J.W. Klop, Process algebra for synchronous communication, Inform. Comput. 60 (1984) 109–137.

[7] J.A. Bergstra, J.W. Klop, Verification of an alternating bit protocol by means of process algebras, in: W. Bibel, K.P. Jantke (Eds.), Spring School on Mathematical Method of Specification and Synthesis of Software Systems, Lecture Notes in Computer Science, vol. 215, Springer, Berlin, 1986, pp. 9–23.

[8] J.A. Bergstra, J.W. Klop, A complete inference system for regular processes with silent moves, in: Proc. Logic Colloquium '86, North-Holland, Amsterdam, 1988, pp. 21–81.

[9] G. Berry, Preemption in concurrent systems, in: Proc. FSTTCS '93, Lecture Notes in Computer Science, vol. 761, Springer, Berlin, 1993, pp. 72–93.

[10] G. Berry, The foundations of Esterel, in: G. Plotkin, C. Stirling, M. Tofte (Eds.), Proof, Language and Interaction: Essays in Honour of Robin Milner, MIT Press, Cambridge, MA, 2000.

[11] G. Berry, The constructive semantics of pure Esterel, Version 3.0, 1999, URL: `http://www.inria.fr/meije/personnel/Gerard.Berry.html`.

[12] G. Berry, G. Gonthier, The Esterel synchronous programming language: Design, semantics, implementation, Sci. Comput. Programming 19 (1992) 87–152.

[13] B. Bloom, S. Istrail, A. Meyer, Bisimulation can't be traced, J. ACM 42 (1995) 232–268.

[14] R. de Simone, A. Ressouche, Compositional semantics of Esterel and verification by compositional reduction, in: Proc. CAV '94, Lecture Notes in Computer Science, vol. 818, Springer, Berlin, 1994, pp. 441–454.

[15] W.J. Fokkink, C. Verhoef, A conservative look at operational semantics with variable binding, Inform. and Comput. 146 (1988) 24–54.

[16] R. van Glabbeek, Bounded nondeterminism and the approximation induction principle in process algebra, in: Proc. STACS '87, Lecture Notes in Computer Science, vol. 247, Springer, Berlin, 1987, pp. 336–347.

[17] G. Gonthier, Sémantique et modèles d'exécution des langages réactifs synchrones; application à Esterel, Thèse d' informatique, Univesité d'Orsay, France, 1988.

[18] J.F. Groote, F. Vaandrager, Structured operational semantics and bisimulation as a congruence, Inform. and Comput. 100 (1992) 202–260.

[19] N. Halbwachs, Synchronous Programming of Reactive Systems, Kluwer Academic Publishers, Dordrecht, 1993.

[20] D. Harel, Statecharts: a visual formalism for complex systems, Sci. Comput. Programming 8 (1987) 231–274.

[21] D. Harel, A. Pnueli, On the development of reactive systems, in: K.R. Apt (Ed.), Logic and Models of Concurrent Systems, NATO, ASI-13, Springer, New York, 1985, pp. 477–498.

[22] R. Keller, Formal verification of parallel programs, Comm. ACM 19 (1976) 371–384.
[23] F. Maraninchi, Operational and compositional semantics of synchronous automaton composition, in: Proc. CONCUR '92, Lecture Notes in Computer Science, vol. 630, Springer, Berlin, 1992, pp. 550–564.
[24] R. Milner, A complete inference system for a class of regular behaviors, J. Comput. System Sci. 28 (1984) 439–466.
[25] R. Milner, Communication and Concurrency, Prentice-Hall, London, 1989.
[26] F. Moller, The importance of the left merge operator in process algebras, in: Proc. ICALP '90, Lecture Notes in Computer Science, vol 443, Springer, Berlin, 1990, pp. 752–764.
[27] D. Park, Concurrency and automata on infinite sequences, in: Proc. Theoretical Computer Science: 5th GI Conference, Lecture Notes in Computer Science, vol. 104, Springer, Berlin, 1981, pp. 167–183.
[28] G. Plotkin, A structural approach to operational semantics, Technical Report DAIMI FN-19, University of Aarhus, Denmark, 1981.
[29] V.A. Saraswat, R. Jagadeesan, V. Gupta, Timed default concurrent constraint programming, J. Symbolic Comput. 11 (1996) 1–46.
[30] T.R. Shiple, G. Berry, H. Touati, Constructive analysis of cyclic circuits, in: Proc. Internat. Design and Testing Conf., IDTC '96, Paris, France, 1996, pp. 328–333.
[31] The Esterel Team, The birth of Esterel, URL: `http://www.esterel.org/Html/History/History.htm`.
[32] S. Tini, Structural operational semantics for synchronous languages, Ph.D. Thesis, Technical Report TD 8-00, University of Pisa, Italy, March 2000.
[33] C. Verhoef, A general conservative extension theorem in process algebra, in: Proc. IFIP Working Conference on Programming Concepts, Methods and Calculi, San Miniato, Italy, IFIP Transactions A-56, Elsevier, Amsterdam, 1994, pp. 149–168.